2004 Version

IPv6 Deployment Guideline

＜DRAFT＞

June 2004

IPv6 Promotion Council of Japan DP-WG

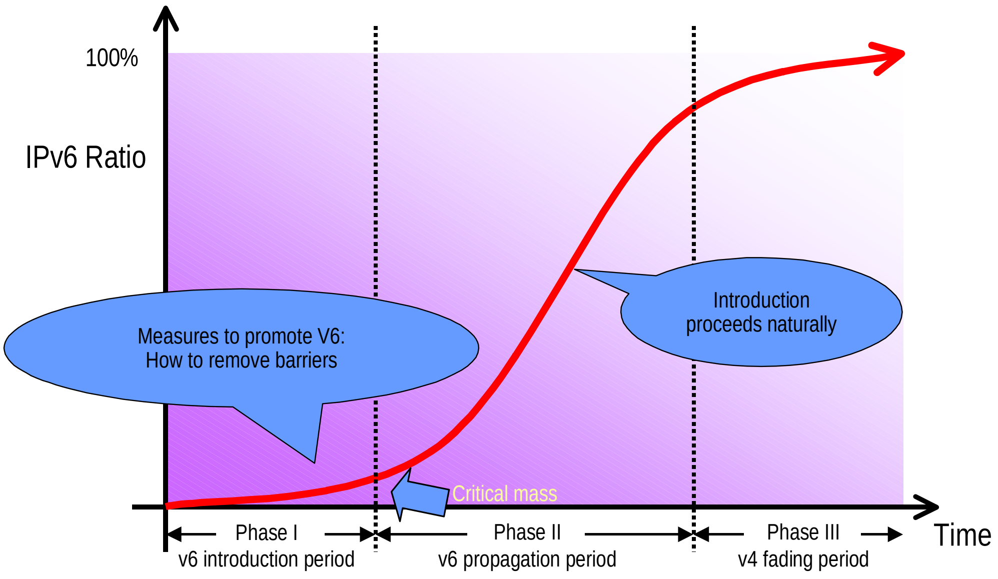
Table of Contents

1. Introduction

1.1 Background: Current Situation with Regard to IPv6 Deployment

1.1.1 Three phases of IPv6 deployment

Three phases of IPv6 deployment



Migration to IPv6 can be explained by dividing the process into three phases (stages). We express these three phases as follows:

Phase 1: IPv6 introduction period
Phase 2: IPv6 propagation period
Phase 3: IPv4 fading period

We currently seem to be at the stage where migration from the phase 1 IPv6 introduction period to the Phase 2 propagation period has begun. It is thought is that this period will involve the greatest energy for IPv6 to move ahead and requires IPv6 promotion measures to remove various barriers from the current conditions. As we pull through this stage, critical mass will arrive soon after and it is thought that IPv6 deployement will proceed on its own.

1.1.2 Barriers to IPv6 deployement

There are three primary obstacles to IPv6 deployement:

1. Don’t know how to do it
2. Still uncomfortable in terms of stability and quality
3. Near-term advantages are difficult to quantify

Of these three primary issues, with regard to the first barrier, people don’t know how to do it, we can implement a workaround, that is, we can prepare a deployement manual for each user entity. Clarifying the deployement process and security model and streamlining of the metric for deployement will certainly be useful in that regard.

With regard to the second barrier, that people are still uncomfortable in terms of stability and quality, it is necessary to verify reliability. Identifying design and operation bugs through demonstration testing and evaluation by tools such as a quality metric can be used to remove such concerns. The IPv6 Promotion Council of Japan, certification working groups and the TAHI project are engaging in various activities to verify mutual connection of various products. These programs greatly contribute to enhancing the feeling of trust.

About the third issue, difficulty quantifying the near-term advantages, it is necessary to show the possibility of new applications through deployement demonstration testing, etc. and to demonstrate cost savings.

1.1.3 Purpose of Part 1

Part 1 is intended to clarify the specific method of IPv6 deployement in response to the first barrier. As a side benefit, Part 1 also reveals how IPv6 can address the issue of the difficulty of quantifying the near-term advantages.

1.2 Structure of Guideline

This guideline consists of two parts. Part 1 is a summary that describes model-independent more general guideline and was created by WG members based on discussions among the members of the IPV6 Promotion Council DP-WG. Part 2 is an implementation that was created based on the IPv6 deployment demonstration experiment project by the Ministry of Internal Affairs and Communications (MIC) for specific cases based on the Summary.

Table 1　Relationship between Part 1 and Part 2

	Part 1　Summary	Part 2　Implementation
Source	IPv6 Promotion Council of Japan DP-WG IPv6 Deployment Guideline	Ministry of Internal Affairs and Communications (MIC) IPv6 Deployement Empirical Experiments IPv6 Deployement Guideline
Features	General Reference	Specific Practical
Description	Deployement scenario, methods are described in variation + advantages and disadvantages	Deployement methods are described based on MIC results
Citations	Feedback the result from Part 2	Scenario and methods cited in Part 1
Handled segments	Home, SOHO, large enterprise and ISP	Local government, large enterprise, small and medium enterprise, home, wireless LAN access and ISP
Schedule	March 2004　2004 version March 2005　2005 version (planned)	March 2004　1st version March 2005　2nd version (planned)

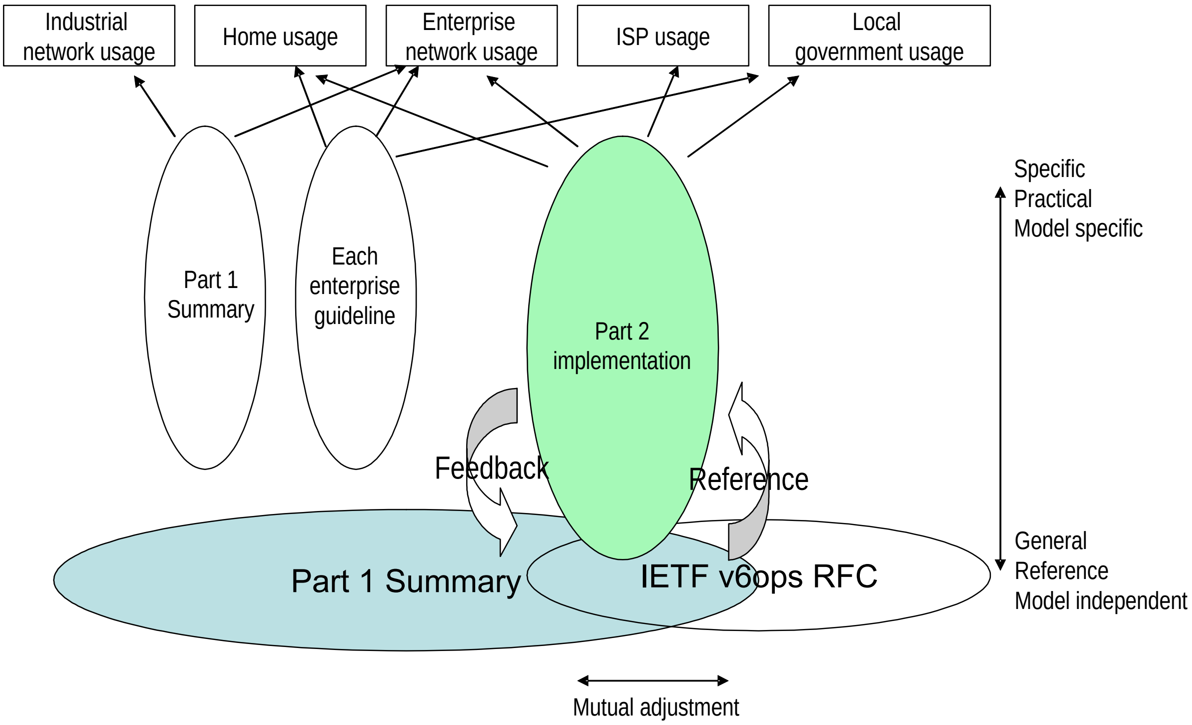


Figure 2: Relationship between Part 1 and Part 2

Part 1 was created through the contributions of a wide range of people and was intended to serve as a guideline for general and reference purposes. Specific router and server models are not listed as preconditions, rather, general functions are assumed throughout. In the same way, when there are multiple deployement methods or implementation methods, other than those cases in which the superiority of one option or another is clear to all concerned parties, to the extent possible we took a neutral stance to clarify the advantages and disadvantages of all possible choices. Because of this, we were able to collect opinions from many people and it became possible to apply the content of the guideline to a wide range of uses.

On the other hand, Part 2 is intended to be a more specific and practical guideline. With respect to descriptions, assumed typical network/system configurations and typical operation policy, we presented detailed deployement methods using specific devices and explained the methodologies together with knowledge obtained through actual demonstration experiments. Therefore, the application range is slightly narrower than Part 1 but the guideline can be said to be more practical because know-how gleaned from actual usage is described.

The two guidelines have the following reference and influence relationship. The Part 2 Implementation guideline is written based on the Part 1 Summary and describes in detail and carefully verifies one of multiple scenarios (or some scenarios). On the contrary, more empirical and specific knowledge written in Part 2 is expected to be fed back to the next version of the Part 1 Summary.

2. Purpose of Part 1

2.1 Structure, Target and Description Scope of Part 1

2.1.1 Segmentation

The major segments Part 1 covers include home networks, SOHO intranets, large enterprise intranets, local government service networks, industrial application networks and ISPs. In this deployement guideline, we discuss home (household) networking, SOHOs, large enterprises and ISPs. Local governments are considered to be part of large enterprises.

The basic principle of Part 1 is to indicate the structure that is possible at this time. We then study the current situation and migration path up to the propagation period. Finally, we screen out issues that need to be resolved during migration. Going beyond simple migration of the current network, we also look for smooth development methods, including new technologies or new applications that may appear before the propagation phase.

2.1.2 Assumed target readers and description scope

The assumed target reader depends on the segment. For the home network, the target readers are service providers and equipment venders for the household market, while for the enterprise network, the target readers are network administrators and system integrators.

Part 1 discusses from the near future up to the propagation period (usage rate of IPv4 and IPv6 is 50-50). Descriptions in the 2004 version (this document) are based on assumption that the near future means within 2004 and that the propagation period is from 2005 to 2006.

The 2005 version is planned to be released within 2004 as a revision of this document.

2.1.3 Description structure in each segment

Definition and characteristics of each segment

① BCP (Best Current Practice)

- Target analysis - modeling
- Now, solution options to deploy IPv6, status that can be applied, advantages and disadvantages

② NW & system form + application that is the target when the situation is 50-50

- Typical device configuration and service types in the home segment during deployement introduction period
- Advantages

③ Issues in the course of 50-50 situation

- Issues that need to be solved
- Requested items to other segments (to ISP, etc.)

④ Security model

- Idea about security
- Implementation of security policies

⑤ Tips

Specific know-how toward introduction of deployement, including:

- Addressing, routing
- Server design
- Network/systems administration
- Security
- Applications
- v4-v6 translator
- Multicast

The guideline for each segment has the above basic structure; however, the actual structure varies according to the characteristics of the segment.

The abbreviation BCP is frequently used in Part 1 and refers to Best Current Practice, which is the best course of action that can be taken at present.

2.2 Deployment Working Group

In May 2003, the IPv6 Promotion Council of Japan established a deployment working group of member volunteers and four groups divided by target segment have been studying issues related to the following two points:

- With respect to migration to introduce IPv6, study the migration introduction model (scenario, cost and architecture) and collect know-how in a Deployement Guide
- In addition, regarding quality management, mutual connectivity and advantages related to the deployement introduction model, we will attempt to reflect the results of the activities of other working groups.

The core members of the Deployement Working Group include:

Chief: Takashi Arano (Intec NetCore, Inc., JPNIC Trustee)
Assistant chief: Hiroaki Sadata (NTT Communications Corporation, IPv6 Promotion Council of Japan)
Akihiro Inomata (Fujitsu Limited, Internet Association Japan IPv6 operation study group chair)
Home SWG Chair: Koji Kubota (Matsushita Electric Industrial Co., Ltd.)
SOHO SWG Chair: Akihiro Inomata (Fujitsu Limited)
Large enterprise/local government SWG Co-Chairs: Yoichi Tsukioka (Hitachi, Ltd.), Hideki Sakanai (NEC Corporation)
ISP SWG Chair: Tetsuya Nakai (NTT Communications Corporation)
Secretariat: Gaku Hashimoto (IPv6 Promotion Council of Japan Secretariat)
(Study members of each SWG are listed in the “Introduction” of each guideline.)

Part 1 is opened as the result of the activities of the Deployment Working Group in 2003. In future, Part 1 will be revised as required.

Inquiries

For questions related to Part 1, please send email to the following address:

IPv6 Promotion Council of Japan DP-WG

wg-dp-comment@v6pc.jp

3. IPv6 Deployment Guideline (Home segment)

3.1 Introduction

This document is intended for vendors who engage in development of household IPv6 equipment and service providers to describe general items, guidelines and methods that need to be considered with regard to adding IPv6 devices to a home network.

The information in this document is intended not as a solution but to offer examples that readers can refer to for advice on specific management policies and constraints on the deployement of IPv6.

3.1.1 SWG Members

Chair

Kubota (Matsushita Electric Industrial Co., Ltd.)

Members (in alphabetical order)

Arano (Intec NetCore, Inc.)
Ishihara (Toshiba Corporation)
Kawashima (NEC Access Technica, Ltd.)
Kikuyama (Matsushita Electric Industrial Co., Ltd.)
Murata (Panasonic Communications Co., Ltd.)
Nakai (NTT Communications Corporation)
Nakamura (Matsushita Electric Industrial Co., Ltd.)
Ogami (Matsushita Electric Industrial Co., Ltd.)
Ozawa (Matsushita Electric Industrial Co., Ltd.)
Sadata (NTT Communications Corporation)
Segawa (Panasonic Communications Co., Ltd.)
Shimada (Matsushita Electric Industrial Co., Ltd.)
Suzuki (Matsushita Electric Industrial Co., Ltd.)
Yamatani (Allies)

3.1.2 Inquiries

For questions related to Part 1, please send email to the following address:

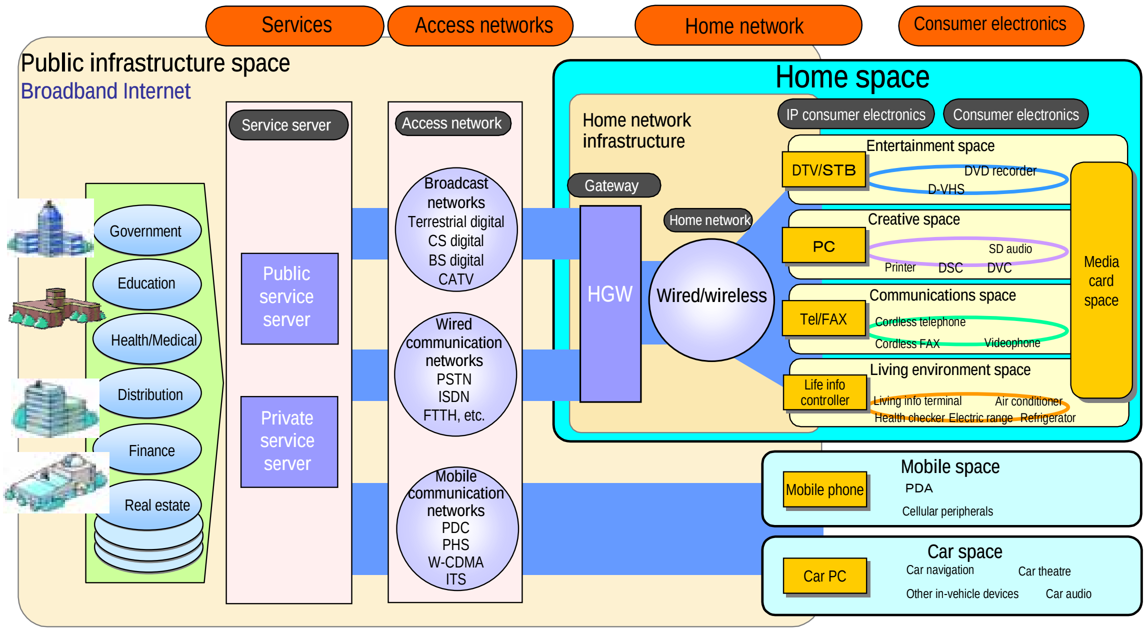
IPv6 Promotion Council of Japan DP-WG

wg-dp-comment@v6pc.jp

3.2 Segment Features

3.2.1 Network Environment Surrounding Homes

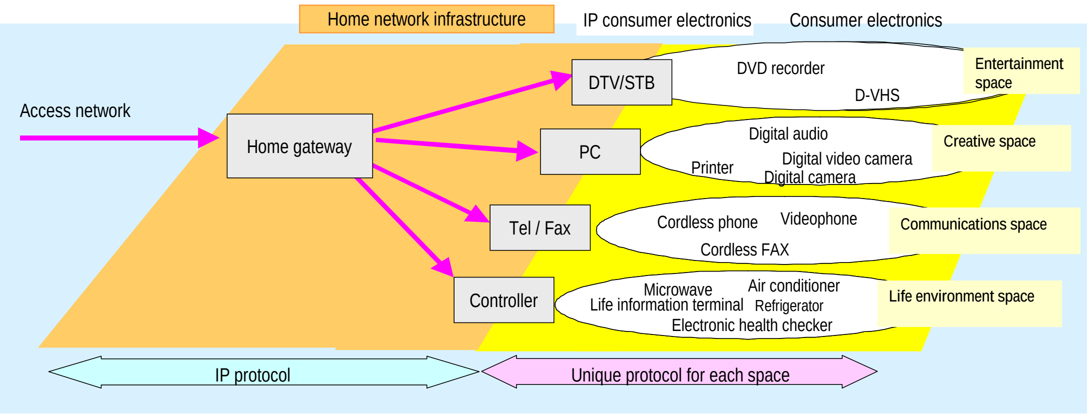
Network environment surrounding homes



Broadband home diffusion in Japan has reached as much as 30 percent and the household is becoming a place where you can connect to the Internet at any time. Connection methods include ADSL, CATV Internet, FTTH and other methods. As the release of net-based consumer electronics is stepped up, the digitization of television broadcasting and the use of Internet phone technology, etc. it is possible that the network will merge into people's lives further. So far, people consciously connect to the Internet for purposes such as information collection. In future, usage styles in which people are not so aware that they are performing data communication may increase. For example, users operate devices at their homes from outside or show still images or home movies at someone’s home. It is certain that Internet-derived services for the general household that are different from conventional PC services may be launched in rapid succession.

3.2.2 Features of Home Segment

Example of home network architecture



- Home gateway (home router) connects to the access network.
- Various protocols (IEEE1394 / USB / Echonet, etc.) are used within each device group.
- In each device group, a device (IP net consumer electronics) that converts IP and individual protocol may exist.
- In future, non-IP devices are expected to use IP.

The following points can be considered to be features of the home segment in future.

- Network structure or devices used are different in each household.
- In addition to PCs, non-PC equipment (white goods such as cleaning equipment, washing machines, refrigerators, air conditioning units, AV equipment, etc.) will also be commonly used.
- No one can manage the network.
- Householder users cannot be expected to configure detailed settings.
- Devices are used with the default settings or settings that the user sets only once.
- Devices, especially consumer electronics, often will not have an interface to configure settings.
- ISP connection services are used.
- For the time being, home networking assumes one segment is in use.
- Basic network needs are not so different from that of the SOHO segment.

In the following descriptions, devices that terminate the IP are discussed and non-IP device/networks (Echonet and IEEE1394, etc.) are not included.

3.2.3 Analysis of Current Situation

Internet connection/usage situation in the current household

The number of subscribers connected to the Internet by connection method are described below. (Statistical data as of December 2003 is provided by the Ministry of Internal Affairs and Communications (MIC))

- Dial-up subscribers: About 19,180,000
- Direct dial-up (PSTN) from PC (modem) or dial-up router ISDN
- Always-on Internet connection subscribers: About 13,640,000
  [ADSL (10,270,000) / FTTH (900,000) / CATV (2,470,000)]
- Internet service subscribers via mobile phone: About 67,800,000

Total number of households in Japan: About 46,000,000 (as of 2000)

Devices used to connect the Internet are mostly routers (home gateway) and PCs and single unit-basis/individual services have begun to be provided for some AV devices. In addition, network services for white goods have been started on an experimental basis by some makers. However, propagation of those services is not expect to be so prevalent in the near future. Furthermore, net cameras and sensor-related devices are beginning to be used but the number of users is still small.

Home network wiring

Home network wiring generally uses Ethernet cable or wireless LAN technologies such as 802.11 a/b/g.

Use of services

General usage of the Internet includes web browsing and mail exchange using mail client software via a mail server such as an ISP. Some hard disk video recorders have functions that allows users to remotely set their devices to record specified programs.

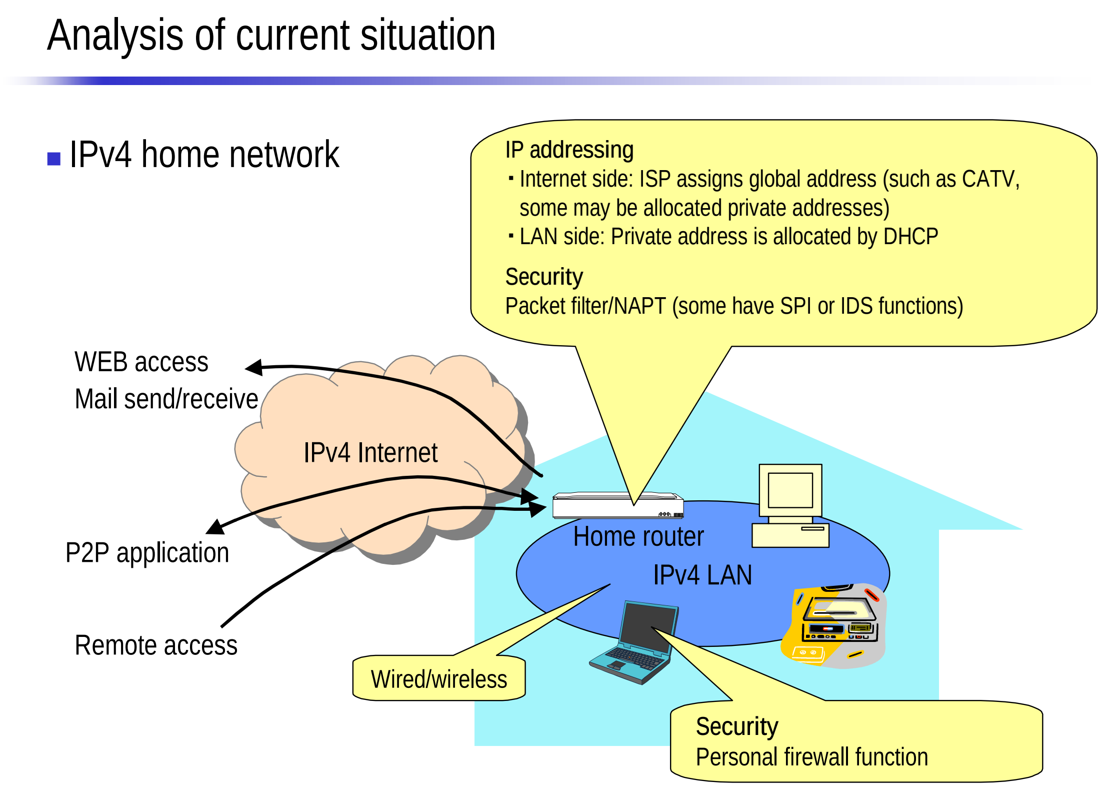
Security

Home network security is currently ensured primarily by routers. The security function of household-use routers is primarily simple security measures such as packet filtering and NAPT function. Some products, however, are equipped with stateful packet inspection or unauthorized access detection functions.

The number of users who install virus checking software in their PCs is increasing significantly and some people use personal firewall products. People have begun using virus check services for mail provided by ISPs.

However, the majority of people use only packet filtering and NAPT based security and do not use functions other than that are already provided.

IPv4 home network



Analysis of current situation

- IPv4 home network

IP addressing
・Internet side: ISP assigns global address (such as CATV, some may be allocated private addresses)
・LAN side: Private address is allocated by DHCP

Security
Packet filter/NAPT (some have SPI or IDS functions)

WEB access
Mail send/receive

IPv4 Internet

P2P application

Remote access

Home router

IPv4 LAN

Wired/wireless

Security
Personal firewall function

The most commonly used network protocol is IPv4, which is used in such a way that one global address is received from an ISP and assigned to a home router. In the home, a private address is assigned by DHCP and the router converts between the private address and global address (with some CATV Internet services, a private address is assigned to the home router as well).

For security, a packet filtering function (and sometimes a firewall function) or a personal firewall function on a PC is used. People use the Web and email and some people actively use file exchange software.

3.2.4 IPv6 Usage in the Home

With this in mind, what trigger will spur such general households to use IPv6? Currently, there are no killer applications or services. Therefore, we discuss triggers that will spur migration to IPv6 based on two aspects: (1) IPv6 terminal development needs for terminal vendors and (2) five Internet usage scenarios at the user side.

IPv6 terminal development needs for terminal vendors

For terminal vendors, the incentive to develop IPv6 terminals is that they will be able to provide the following services.

① Broadcast type services

Service providers provide broadcasting-like services and users must have a terminal to receive the service. Examples of such closed services include video broadcasting, remote maintenance, remote monitoring, meter-reading, etc.

② Heavy user type

As IP users begin to take advantage of IPv6, special terminals become necessary as an extension of user needs. Home servers, VTR, chat, and videoconferencing are some examples of this type of usage.

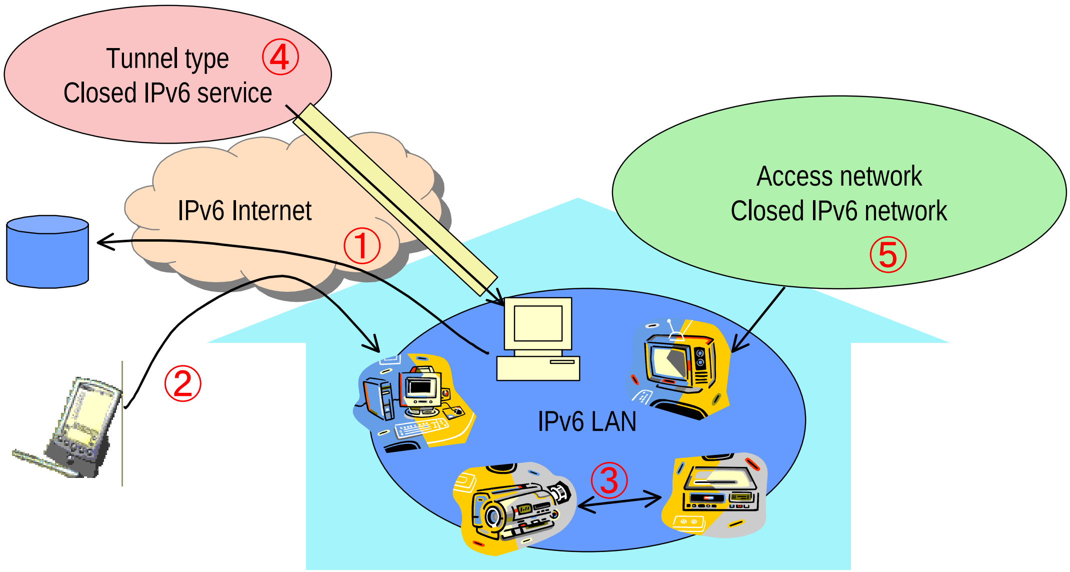
③ Inter-household communication type

IPv6 protocol is introduced for communication between consumer electronics. In this case, usage is not limited to within the home. It is thought that device vendors will voluntarily develop terminals that use IPv6. Communication is realized between cameras and printers, cameras and TVs, TV chat terminals, refrigerators and TVs, etc.

IPv6 usage scenarios on the user side

Clarification of characteristics of IPv6 usage scene

- Five assumed usage scenes



As shown in the above figure, five usage scenarios are discussed in this section.

① Connectivity to the world similar to IPv4
Primarily Web access, mail, image viewing by WMP
New style applications include web access, firmware updates, etc. from white goods

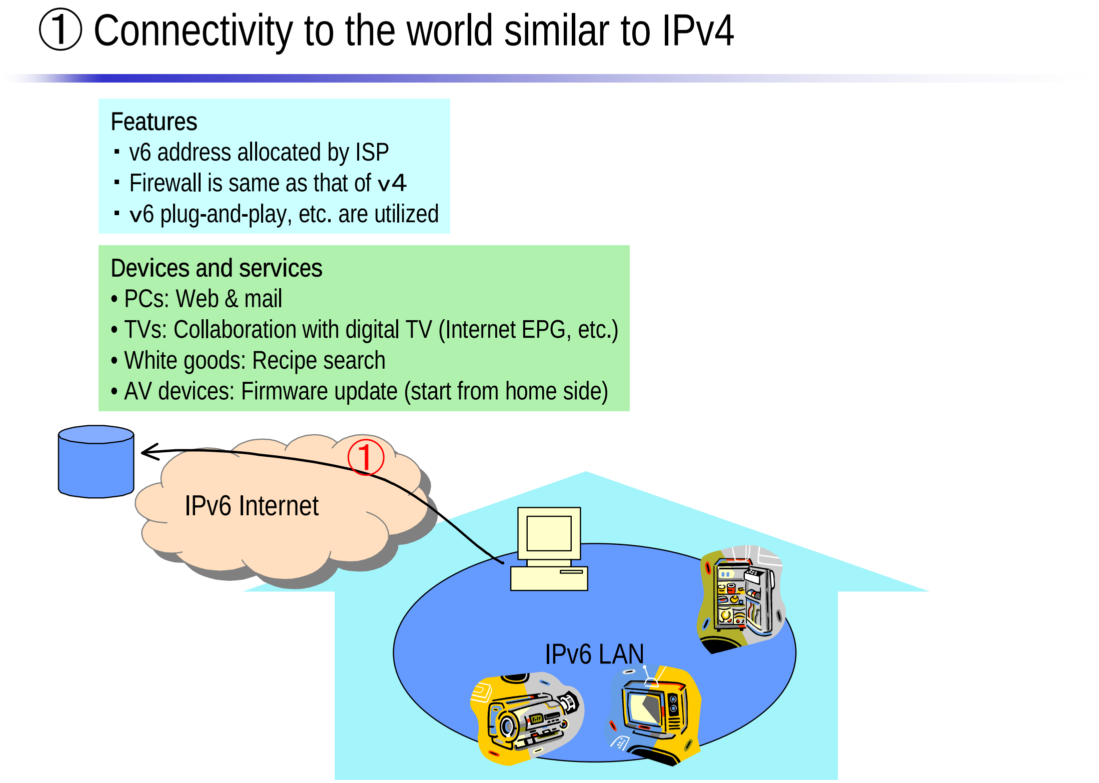
② Access from outside to inside (individuals use IPv6 by choice)
Home video server access, Web cameras, air conditioning operation, etc.

③ Communication between devices on a LAN (consumer electronics makers select IPv6)
Connection between TV and video, video chat between relatives using Internet + VPN

④ Provisioning of tunnel-based remote services (service operators provide IPv6)
Remote device maintenance, text broadcasting on TVs, local government service with special devices, etc.

⑤ Closed services within access network (line providers provide IPv6)
TV video distribution via multicast, critical communication with guaranteed QoS.

① Connectivity to the world similar to IPv4



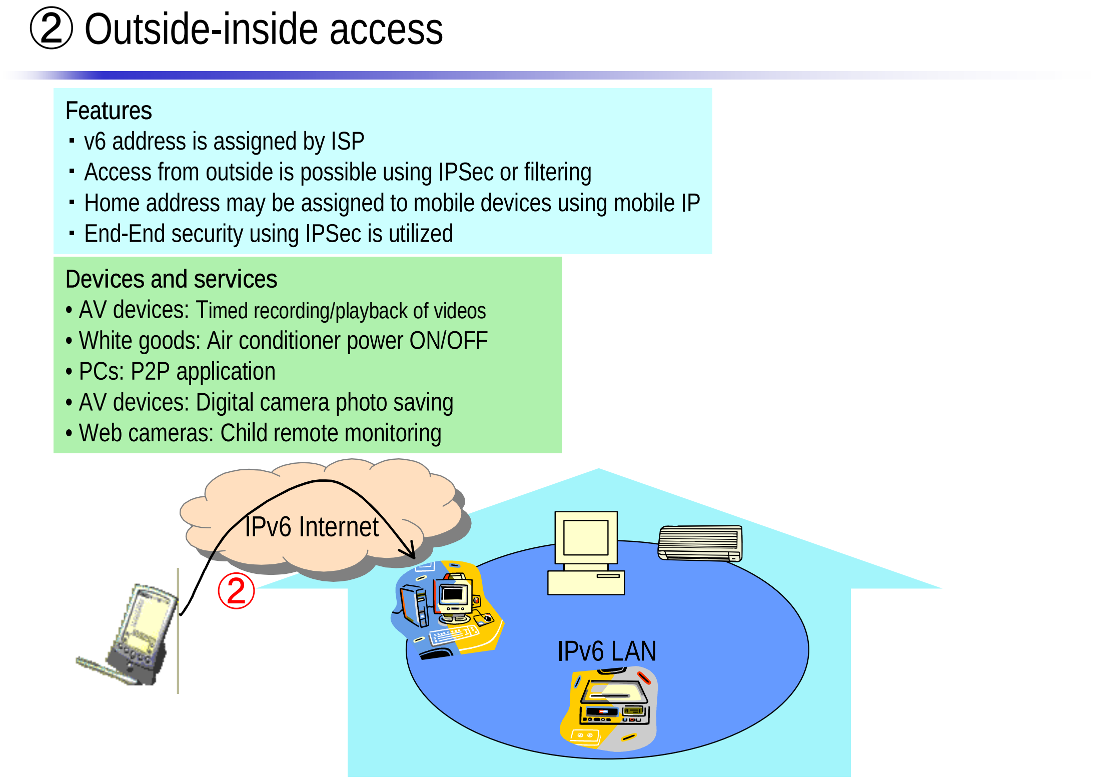
① Connectivity to the world similar to IPv4

Features
- v6 address allocated by ISP
- Firewall is same as that of v4
- v6 plug-and-play, etc. are utilized

Devices and services
- PCs: Web & mail
- TVs: Collaboration with digital TV (Internet EPG, etc.)
- White goods: Recipe search
- AV devices: Firmware update (start from home side)

With this type of usage, applications similar to those used with the current IPv4 can be assumed. These applications include Web and electronic mail via a PC, collaboration with digital TV such as Internet EPG with TV, recipe searches with white goods and firmware updates for AV devices (initiated from the home side). In order to provide these services with IPv6, an IPv6 address assigned by the ISP is used and in some cases, the IPv6 plug-and-play function is used.

② Outside-inside access



② Outside-inside access

Features

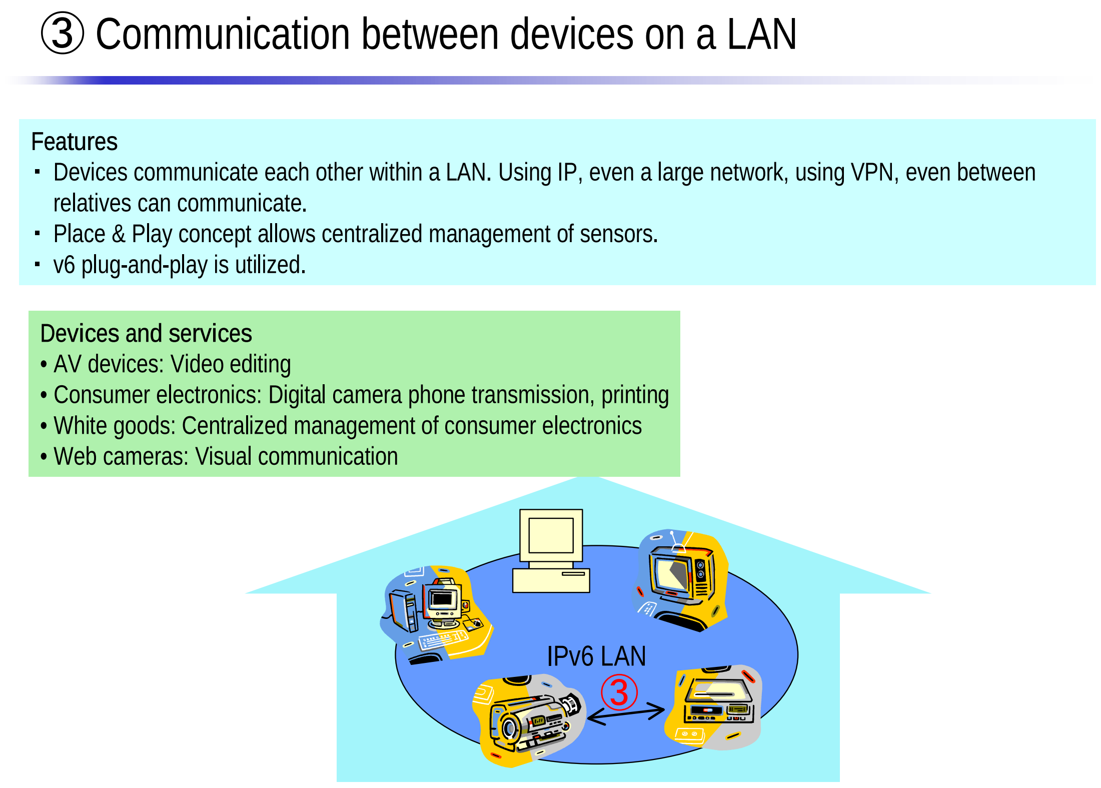
- v6 address is assigned by ISP
- Access from outside is possible using IPSec or filtering
- Home address may be assigned to mobile devices using mobile IP
- End-End security using IPSec is utilized

Devices and services

- AV devices: Timed recording/playback of videos
- White goods: Air conditioner power ON/OFF
- PCs: P2P application
- AV devices: Digital camera photo saving
- Web cameras: Child remote monitoring

This type of usage is often talked about as an advantage of IP consumer electronics. Applications include timed recording/playback of videos, photo storage from digital cameras, turning air conditioner power ON/OFF, P2P applications for PCs, and remote monitoring of children via web cameras. In this case, security needs to be ensured by IPsec or filtering settings. IPsec is used with devices on a house end-to-end basis. In some cases, mobile IP may be used.

③ Communication between devices on a LAN



③ Communication between devices on a LAN

Features

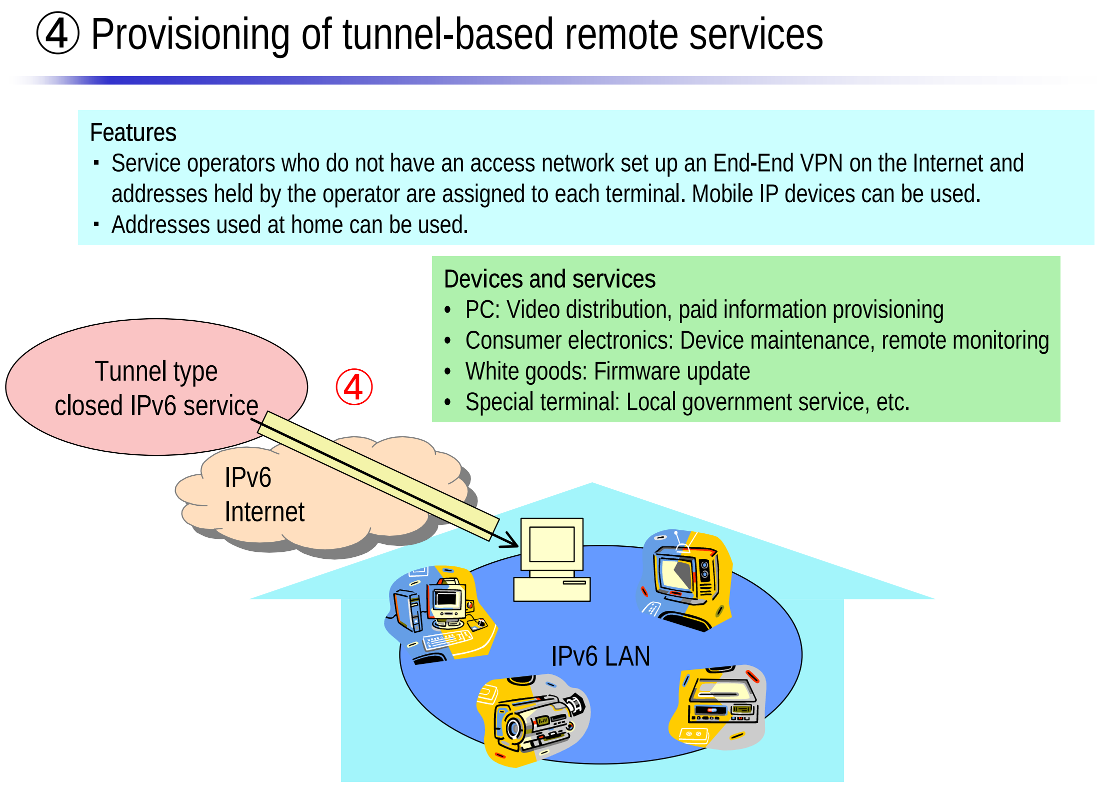
- Devices communicate each other within a LAN. Using IP, even a large network, using VPN, even between relatives can communicate.
- Place & Play concept allows centralized management of sensors.
- v6 plug-and-play is utilized.

Devices and services

- AV devices: Video editing
- Consumer electronics: Digital camera phone transmission, printing
- White goods: Centralized management of consumer electronics
- Web cameras: Visual communication

In a household, connecting consumer electronics via a network generates new applications such as video editing, printing from digital camera, centralized management of white goods, etc. In that case, a LAN means the home, and using VPN technology that provides connections between household allows us to, for example, communicate with relatives using Web video cameras. With the same connection, centralized management of sensors is possible.

④ Provisioning of tunnel-based remote services



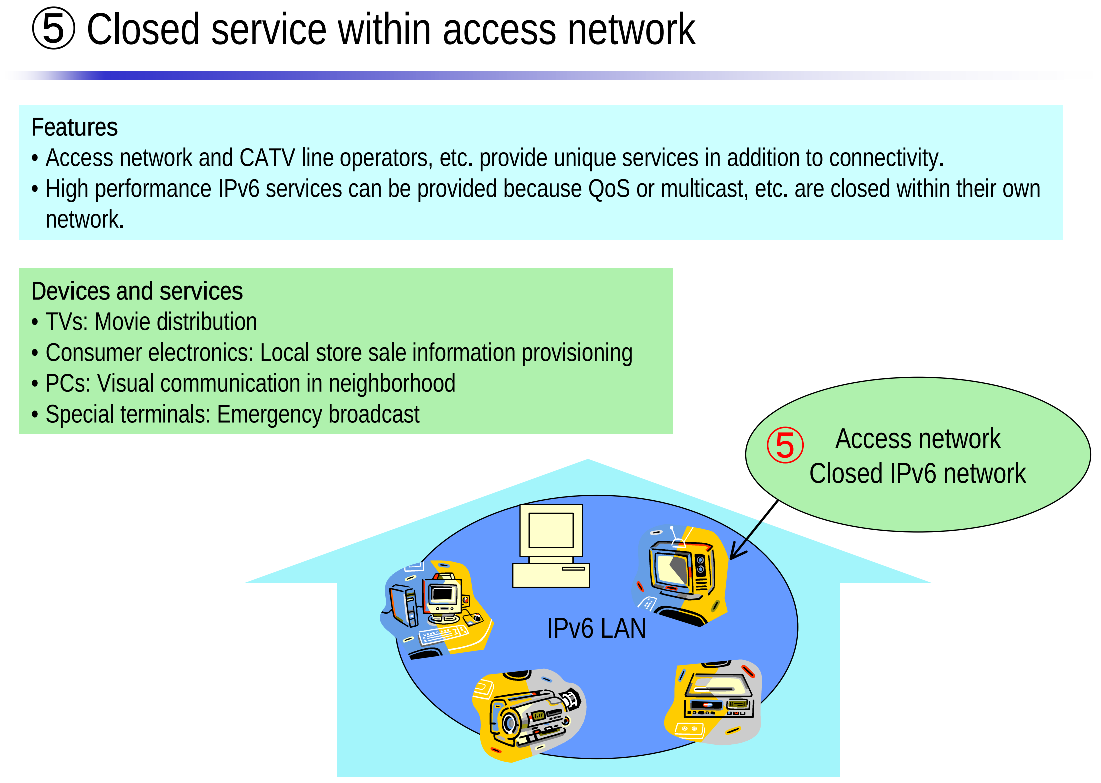
④ Provisioning of tunnel-based remote services

Features
- Service operators who do not have an access network set up an End-End VPN on the Internet and addresses held by the operator are assigned to each terminal. Mobile IP devices can be used.
- Addresses used at home can be used.

Devices and services
- PC: Video distribution, paid information provisioning
- Consumer electronics: Device maintenance, remote monitoring
- White goods: Firmware update
- Special terminal: Local government service, etc.

It is possible that operators who do not own access networks may use IPv6 for their services. These services may include video distribution to PCs, provisioning of pay information, consumer electronics maintenance, remote monitoring, firmware update of white goods and provisioning of local government services using special terminals. For the network configuration in such cases, end-to-end VPN is set on the Internet without changing the user's IPv6 address or mobile IP is used to grant an address held by the operator on a single terminal basis.

⑤ Closed service within access network



⑤ Closed service within access network

Features
- Access network and CATV line operators, etc. provide unique services in addition to connectivity.
- High performance IPv6 services can be provided because QoS or multicast, etc. are closed within their own network.

Devices and services
- TVs: Movie distribution
- Consumer electronics: Local store sale information provisioning
- PCs: Visual communication in neighborhood
- Special terminals: Emergency broadcast

⑤ Access network
Closed IPv6 network

With this type usage, line operators such as access networks and CATV provide unique services in addition to connectivity to the world. In that case, QoS, multicast, etc. are closed within the network and it is possible to provide high-performance IPv6 services. Applications include movie distribution, delivery of sale information of neighborhood stores to TVs and the broadcast of emergency information via special terminals.

3.2.5 Deployement Model Toward Usage Scenarios

This section discusses how to migrate to IPv6 and the issues within the five usage scenarios. Roughly speaking, the following issues should be pointed out:

With regard to scenario ①, it is natural that things that can be done with IPv4 can also be done with IPv6. About scenario⑤, this type of usage may be prominent as a form of service in the immediate future. There are two possibilities for scenario ③. In one, devices are physically connected, while in the other they are connected virtually over the same LAN via a VPN. It is desirable to implement both types of connection. Technically, if the issues in scenario ② can be solved, we believe that the issues in all usage scenarios can be solved.

In the home segment, what does a 50-50 ratio of IPv4 and IPv6 usage look like? IPv4 and IPv6 devices coexist in homes. Applications include not only Web access and email but also encompass services and applications that are based on collaboration between devices in homes. Also, work must be begun on services and applications that allow users to operate or monitor devices in their houses remotely and it is expected that services will be provided in which to the maximum extent possible users are unaware of which protocol is being used (IPv4 or IPv6). When aiming for a 50-50 ratio, you must address the issues in scenario ②. This is discussed in the next section.

3.3 Deployement Models and Scenarios

3.3.1 Ideas about Deployement Models and Scenarios

In this section, the following three models are assumed to represent current household configurations.

- Multiple devices are connected by a router
- Only one terminal is connected (bridge connection) by a modem (dial-up, ADSL modem, media converter)
- No network devices

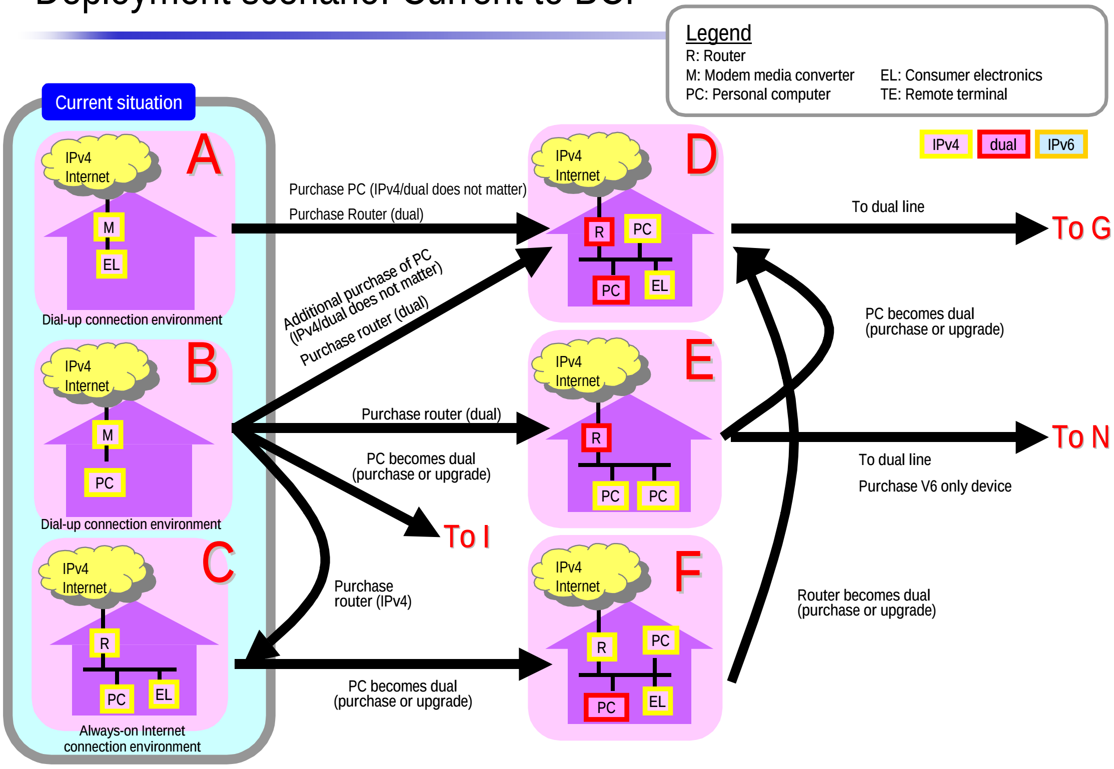
Basically we are considering a scenario of IPv6 deployement in which PC and non-PC devices coexist. There are many issues common to the SOHO segment but usage forms centered on non-PC devices are characteristic of households. We assume household models in a BCP 50-50 situation and clarify the differences between models to identify issues that will arise during IPv6 deployement.

As shown below, the entire deployement image can be expressed using three deployement scenarios. These scenarios do not necessarily cover every possible model we can think of and/or it is not necessary to go through each of the steps in the order.

However, basically, the mainstream scenario is supposed to be the one that includes Models A, B or C (current condition) and D and then moves on to models K and L (50-50) via Model G (BCP). However, this is not so different from issues in the SOHO segment or general migration to IPv6.

As a non-mainstream scenario in the home segment, households with no PC follow a J→M→O deployement scenario with consumer electronics and game machines. Also, as a development case when only those items inside a home are networked, P→{M,H}→{K,L,O} can be considered.

Deployment scenario: Current to BCP



Legend
R: Router
M: Modem media converter
PC: Personal computer
EL: Consumer electronics
TE: Remote terminal

IPv4 dual IPv6

Current situation

A
IPv4 Internet
M
EL
Dial-up connection environment

B
IPv4 Internet
M
PC
Dial-up connection environment

C
IPv4 Internet
R
PC EL
Always-on Internet connection environment

Purchase PC (IPv4/dual does not matter)
Purchase Router (dual)

Additional purchase of PC (IPv4/dual does not matter)
Purchase router (dual)

Purchase router (dual)

PC becomes dual (purchase or upgrade)

To I

Purchase router (IPv4)

PC becomes dual (purchase or upgrade)

D
IPv4 Internet
R PC
PC EL

E
IPv4 Internet
R
PC PC

F
IPv4 Internet
R PC
PC EL

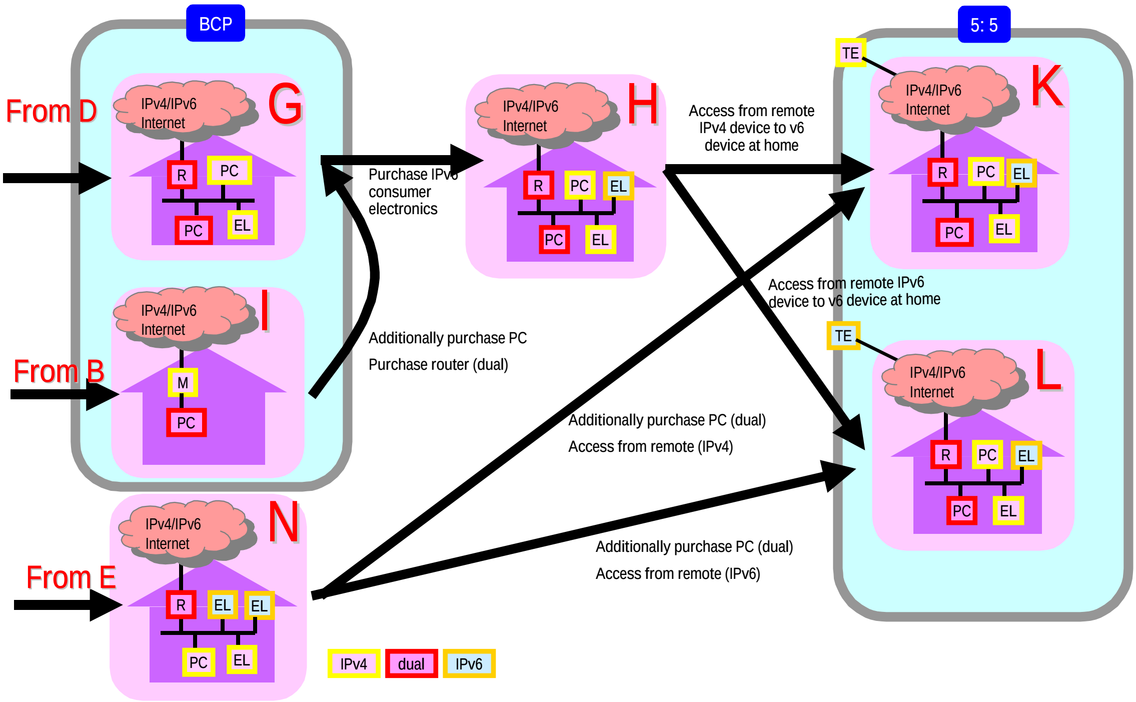
To dual line
To G

PC becomes dual (purchase or upgrade)

To N
To dual line
Purchase V6 only device

Router becomes dual (purchase or upgrade)

Deployment scenario: BCP to 50-50



BCP

From D
G
IPv4/IPv6 Internet
R PC
PC EL

From B
I
IPv4/IPv6 Internet
M
PC

From E
N
IPv4/IPv6 Internet
R EL EL
PC EL

Purchase IPv6 consumer electronics

Additionally purchase PC
Purchase router (dual)

H
IPv4/IPv6 Internet
R PC EL
PC EL

Access from remote IPv4 device to v6 device at home

Access from remote IPv6 device to v6 device at home

Additionally purchase PC (dual)
Access from remote (IPv4)

Additionally purchase PC (dual)
Access from remote (IPv6)

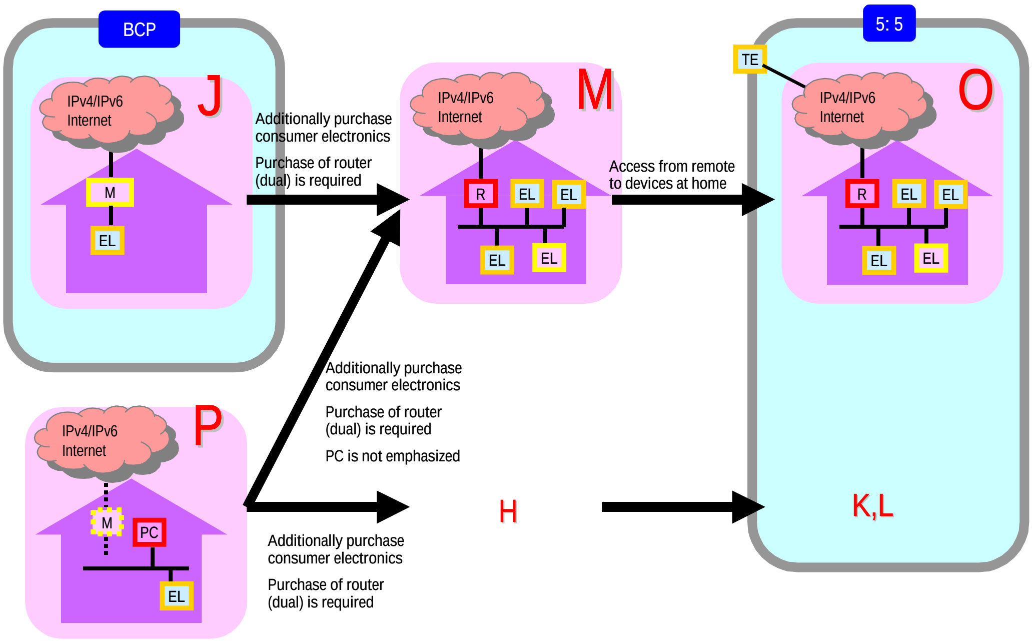
5: 5

TE
K
IPv4/IPv6 Internet
R PC EL
PC EL

TE
L
IPv4/IPv6 Internet
R PC EL
PC EL

IPv4 dual IPv6

Deployment scenario: non-PC model



Additionally purchase consumer electronics

Purchase of router (dual) is required

Access from remote to devices at home

Additionally purchase consumer electronics

Purchase of router (dual) is required

PC is not emphasized

Additionally purchase consumer electronics

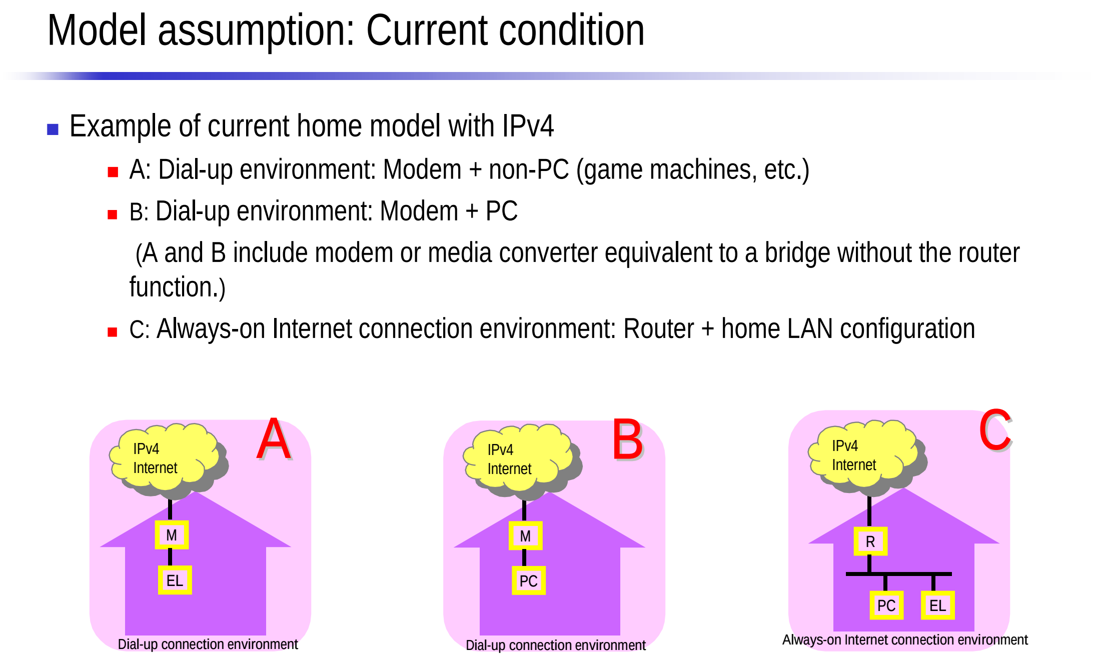
Purchase of router (dual) is required

3.3.2 Assumptions of Each Model

Each model is defined by the following items.

- Configuration (devices in the home network and connection point with the Internet)
- Applications used (applications used in households)
- Addressing system (assignment of addresses)
- Naming (query/registration method)
- Security measures (encryption, prevention of unauthorized access, virus measures, DoS measures)
- Setting method (device setting methods)

Model assumption: Current condition



Model assumption: Current condition

- Example of current home model with IPv4
  - A: Dial-up environment: Modem + non-PC (game machines, etc.)
  - B: Dial-up environment: Modem + PC
    (A and B include modem or media converter equivalent to a bridge without the router function.)
  - C: Always-on Internet connection environment: Router + home LAN configuration

A
IPv4 Internet
M
EL
Dial-up connection environment
B
IPv4 Internet
M
PC
Dial-up connection environment
C
IPv4 Internet
R
PC
EL
Always-on Internet connection environment

About the current home situation, the following three models can be assumed.

A: Dial-up environment: Modem + Non PC (game machines, etc.)
B: Dial-up environment: Modem + PC
C: Always-on Internet connection environment: Router + home LAN configuration

Modems used in models A and B include modems or media converters equivalent to a bridge without a router function.

Features of Model A

Model		A: Single function model
Description		One device in home
Configuration	Boundary with network	Modem or MediaConverter (bridge connection)
	Connected devices	Game machine, non-PC devices (AV device, IP cameras, IP phones, etc.)
Applications used		Net games, remote VTR timed recording (set via mobile phone)
Address	Internet side	Global IP by DHCP or PPP
	Local side	---
Naming	Query	(In→Out) DNS server specified by ISP (Out→In) DDNS service or special server provided by vendor is used
	Registration	External: DDNS or special server provided by vendor
Security measure	Encryption	Handled for device/application individually
	Measures to prevent unauthorized access	Handled for device/application individually
	Virus measures	Handled for device/application individually
	DoS measures	Handled for device/application individually
Setting method		None
Other		

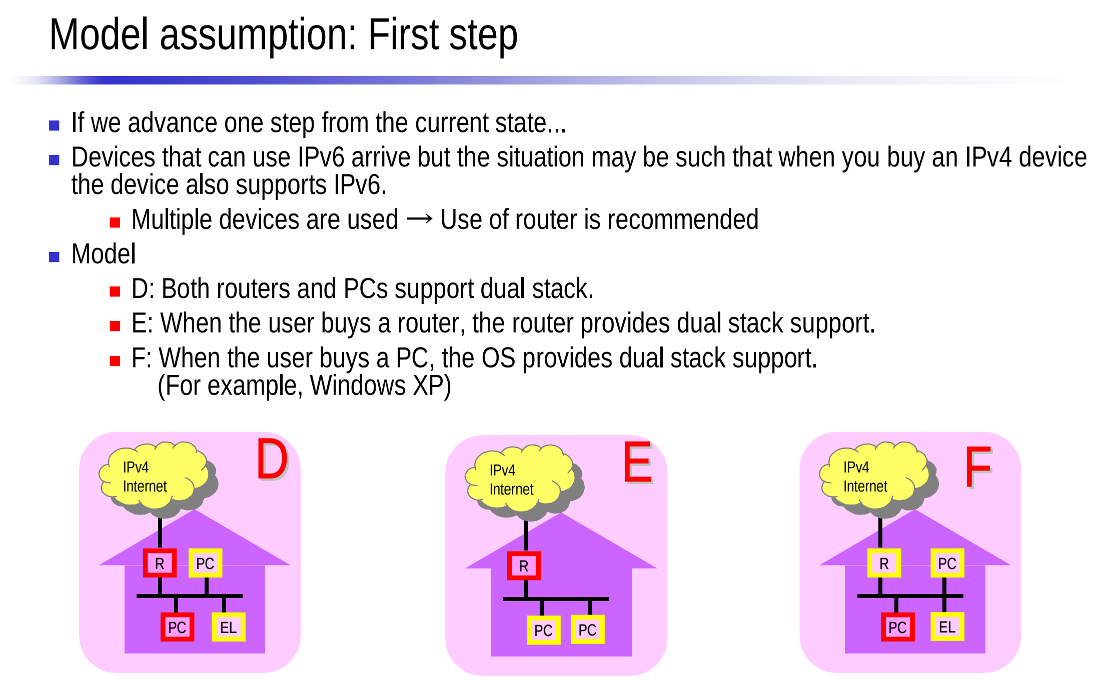
Features of Model B

Model		B: PC only model
Description		One PC at home
Configuration	Boundary with network	Modem or MC (bridge connection)
	Connected devices	PC
Applications used		Mail, Web, Net games, connected to company Intranet
Address	Internet side	Global IP by DHCP or PPP
	Local side	---
Naming	Query	(In→Out) DNS server specified by ISP (Out→In) DDNS service or special server provided by vendor is used
	Registration	External: DDNS or special server provided by vendor
Security measure	Encryption	Handled for device/application individually
	Measures to prevent unauthorized access	Personal firewall
	Virus measures	Virus checker, service provided by ISP
	DoS measures	Personal firewall
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		

Features of Model C

Model		C: IPv4 network
Description		Multiple PCs/devices in home
Configuration	Boundary with network	Router connection
	Connected devices	PC, game machine, non-PC devices (AV, consumer electronics, IP cameras, IP phones)
Applications used		Mail, Web, Net games, connected to company Intranet
Address	Internet side	Global IP by DHCP or PPP (usually fixed)
	Local side	DHCP
Naming	Query	(In→Out) DNS server specified by ISP, relay by router for home (Out→In) DDNS service or special server provided by vendor is used Settings are required to go beyond the router (In→In) NETBIOS
	Registration	External: DDNS or special server provided by vendor is used
Security measure	Encryption	Router (PPTP, IPsec: termination or through)
		Handled for device/application individually
	Measures to prevent unauthorized access	Handled by router, personal firewall
	Virus measures	Virus checker, service provided by ISP
	DoS measures	Handled by router, personal firewall
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		

(2) Model assumption: First step



Model assumption: First step

- If we advance one step from the current state...
- Devices that can use IPv6 arrive but the situation may be such that when you buy an IPv4 device the device also supports IPv6.
  - Multiple devices are used → Use of router is recommended
- Model
  - D: Both routers and PCs support dual stack.
  - E: When the user buys a router, the router provides dual stack support.
  - F: When the user buys a PC, the OS provides dual stack support.
    (For example, Windows XP)

As one step advanced from the above three models, a situation can be imagined in which a device that can also use IPv6 appears on the market and the user happens to buy it and, though it comes with IPv6, the user only uses the device with IPv4 networks. For example, when multiple devices are used by dial-up users, many people may begin using routers and the routers will begin to support IPv6; however, at this stage, though the IPv6 function begins to enter the household it does not mean IPv6 is actually used.

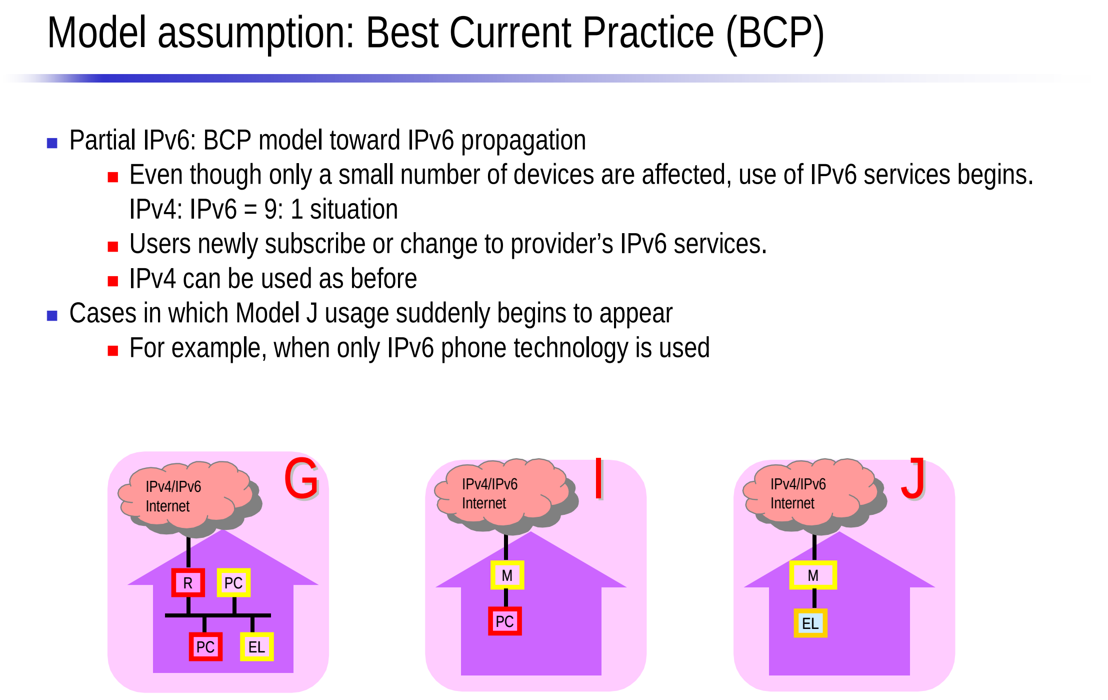
D: Both the router and PC support dual stack
E: When the user buys a router, the router provides dual stack support.
F: When the user buys a PC, the OS provides dual stack support.
(For example, Windows XP)

Features of Model D

Models E and F are basically the same as Model D, thus are omitted.

Model		D: Router/PC is dual but is always used with IPv4
Description		Multiple PCs/devices in home
Configuration	Boundary with network	Router connection
	Connected devices	PC, game machine, non-PC devices (AV, consumer electronics, IP cameras, IP phones)
Applications used		Mail, Web, Net games, connected to company Intranet, remote VTR timed recording
Address	Internet side	Global IP by DHCP or PPP (usually fixed)
	Local side	DHCP
Naming	Query	Same as Model C
	Registration	Same as Model C
Security measure	Encryption	Router (PPTP, IPsec: termination or through) Handled for device/application individually
	Measures to prevent unauthorized access	Handled by router, personal firewall
	Virus measures	Virus checker, service provided by ISP
	DoS measures	Handled by router, personal firewall
Setting methods		Windows applications, unique setting method for each application, auto setting, update
Other		

Model assumption: Best Current Practice (BCP)



Model assumption: Best Current Practice (BCP)

- Partial IPv6: BCP model toward IPv6 propagation
  - Even though only a small number of devices are affected, use of IPv6 services begins. IPv4: IPv6 = 9: 1 situation
  - Users newly subscribe or change to provider’s IPv6 services.
  - IPv4 can be used as before
- Cases in which Model J usage suddenly begins to appear
  - For example, when only IPv6 phone technology is used

With respect to BCP, at this stage only certain users use IPv6 services. The IPv4:IPv6 ratio is 9:1. At this point, users either subscribe to an IPv6 service provider or change to IPv6 service with their existing provider. IPv4 can also be used as before. It can be imagined that some people will start connecting to the Internet only to use IP phone technology and the phone will happen to be an IPv6 phone. In this case, use of IPv6 begins with Model J.

Features of Model G

(The IPv4 section is same as for Model C and D.)

Model		G: Only PC uses IPv6 and others use IPv4
Description		Multiple PCs/devices in home, some PCs are dual
Configuration	Boundary with network	Router (dual) connection
	Connected devices	PCs, game machines, non-PC devices (AV, consumer electronics, IP cameras, IP phones)
Applications used		WEB, connected to company Intranet?
Address	Internet side	/48/64prefix, DHCPv6, 6to4 auto generation, configured, DTCP
	Local side	Prefix is notified by RA, Link-local
Naming	Query	Under current conditions, there are problems with Windows XP-IPv6.
	Registration	
Security measures	Encryption	Router, Windows XP (null coding IPsec)
	Measures to prevent unauthorized access	Packet filter by router. SPI Standard Windows XP support, v6 personal firewall is not yet implemented.
	Virus measures	Virus checker
	DoS measures	No special measures
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		

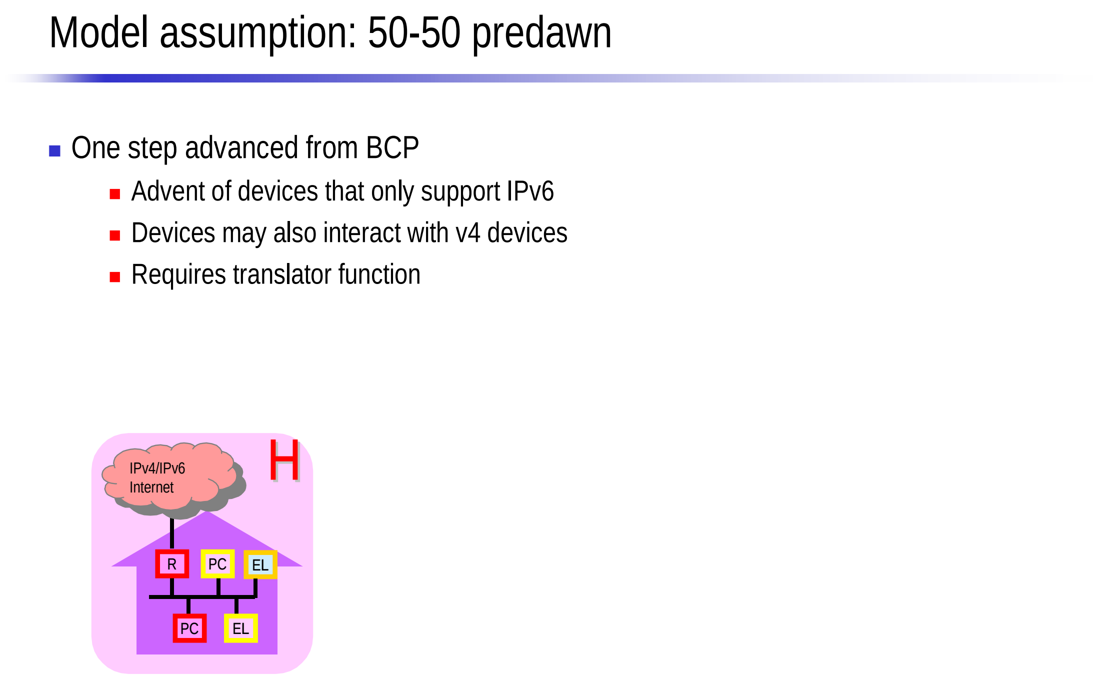
Features of Model I

Model		I: Same as B's status; only the PC is replaced with a dual model.
Description		One PC/device in home, PC is a dual model
Configuration	Boundary with network	Modem or MC (bridge connection)
	Connected devices	PC
Applications used		Connected to Internet and closed network (Flet's Square, etc.) WEB, connected to company Intranet?
Address	Internet side	(IPv4) Global IP address is received by DHCP or PPP, one address
	Local side	(IPv6) Prefix is notified by RA, Link-local
Naming	Query	DNS server specified by ISP, DDNS is used from outside
	Registration	External: DDNS
Security measure	Encryption	Windows XP (null coding IPsec)
	Measures to prevent unauthorized access	Standard Windows XP support, requires a v6 personal firewall.
	Virus measures	Requires a v6 virus checker v6, handled by ISP
	DoS measures	Handled by personal firewall
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		This model is meaningful when the application only provides v6 support. If not, only the v4 environment is used and users may not be aware of v6 matters.

Features of Model J

Model		J: All-in-one consumer electronics packages
Description		One v6 consumer electronics device in home
Configuration	Boundary with network	Modem or MC (bridge connection)
	Connected devices	v6 only consumer electronics, IP phones
Applications used		Telephone, timed video recording
Address	Internet side	-
	Local side	Prefix is notified by RA (when authentication takes place, RA cannot be performed) Link-local
Naming	Query	External: DDNS, SIP server for telephone, special name server provided by vendor
	Registration	
Security measure	Encryption	Left to **x**SP. Is it possible for an end device to be equipped with an encryption chip?
	Measures to prevent unauthorized access	
	Virus measures	
	DoS measures	
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		In combination with consumer electronics, telephones, timed video recordings, etc. are used as xSP services. Security and addressing to end devices are provided as xSP-based services.

Model assumption: 50-50 predawn



Model assumption: 50-50 predawn

- One step advanced from BCP
  - Advent of devices that only support IPv6
  - Devices may also interact with v4 devices
  - Requires translator function

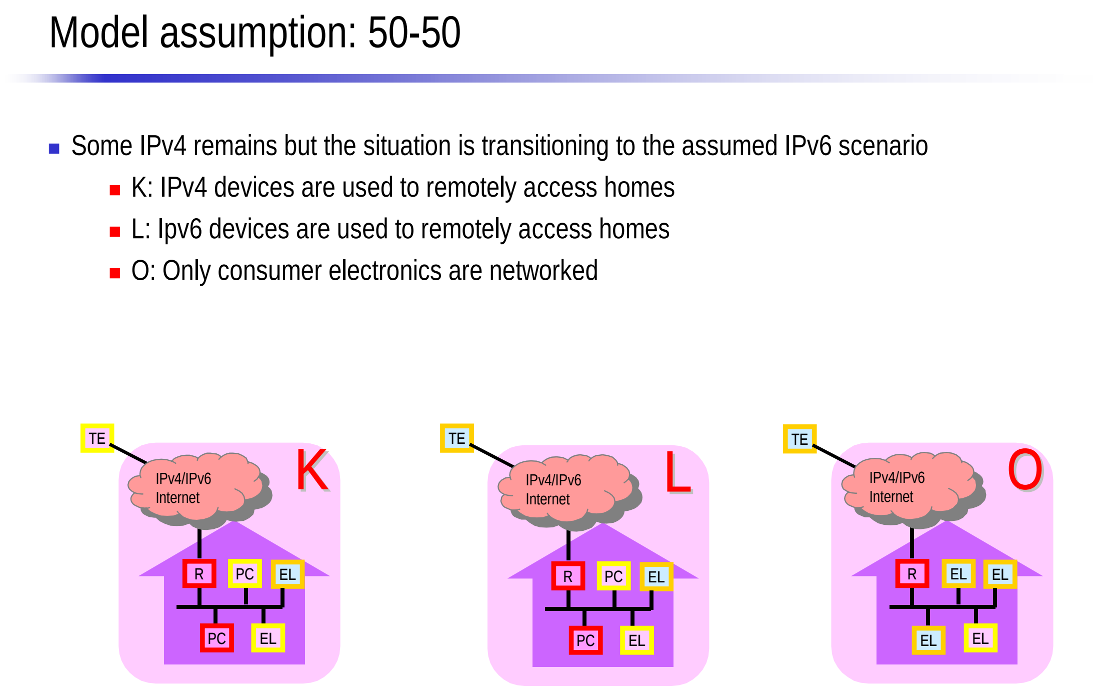
Before the ratio reaches 50-50, devices such as IP phones may appear that only support IPv6 but that can also interact with IPv4 devices. At that time, it is necessary to place a function somewhere to convert between the two protocols.

Features of Model H

(The IPv4 section is the same as that of Models C and D.)

Model		H: In addition to condition G, devices that only support IPv6 are added.
Description		Multiple PCs/devices in home, some PCs are dual, some support v6 only
Configuration	Boundary with network	Router (dual) connection
	Connected devices	PCs, game machines, non-PC devices (AV, consumer electronics, IP cameras, IP phones)
Applications used		Web, connected to company Intranet, v6 devices communicate with each other at home
Address	Internet side	/48/64prefix, DHCPv6, 6to4 auto generation, configured, DTCP
	Local side	Prefix is notified by RA, Link-local
Naming	Query	(In→In) DNS-relay, DDNS is registered individually, uPnP-v6
	Registration	Under current conditions, there are problems with Windows XP-IPv6.
Security measure	Encryption	Router, Windows XP (null coding IPsec)
	Measures to prevent unauthorized access	Packet filter by router. SPI Standard Windows XP support, progress is being made toward adoption of v6 personal firewalls
	Virus measures	Virus checker
	DoS measures	No special measures
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		The location of the translator need to be studied.

Model assumption: 50-50



Model assumption: 50-50

- Some IPv4 remains but the situation is transitioning to the assumed IPv6 scenario
  - K: IPv4 devices are used to remotely access homes
  - L: Ipv6 devices are used to remotely access homes
  - O: Only consumer electronics are networked

With the 50-50 situation, some IPv4 usage remains. However, the IPv6 usage scene assumed at the beginning of this document is realized. The following three methods can be imagined:

K: IPv4 devices are used to remotely access homes
L: IPv6 devices are used to remotely access homes
O: Only consumer electronics are networked

Features of Model K

Model		K: Condition H **+** v4 devices remotely access devices in home
Description		Multiple PCs/devices in home, some PCs are dual, some are v6 only, external devices are v4
Configuration	Boundary with network	Router (dual) connection
	Connected devices	PCs, game machines, non-PC devices (AV, consumer electronics, IP cameras, IP phones) v4 external devices (mobile phones, PCs (PDA))
Applications used		Set VTR timed recordings from mobile phones, use external devices to view camera images inside the home.
Address	Internet side	/48/64prefix, DHCPv6, 6to4 auto generation, configured, DTCP
	Local side	Prefix is notified by RA, Link-local
Naming	Query	Same as H
	Registration	
Security measure	Encryption	Router, Windows XP (null coding IPsec)
	Measures to prevent unauthorized access	Packet filter by router. SPI Standard Windows XP support, v6 personal firewall is not yet implemented.
	Virus measures	Virus checker, use of services provided by ISP
	DoS measures	No special measures
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		It is recommended that the translator function be implemented on the router. When connecting up to the router with IPv4, detailed router settings are required.

Features of Model L

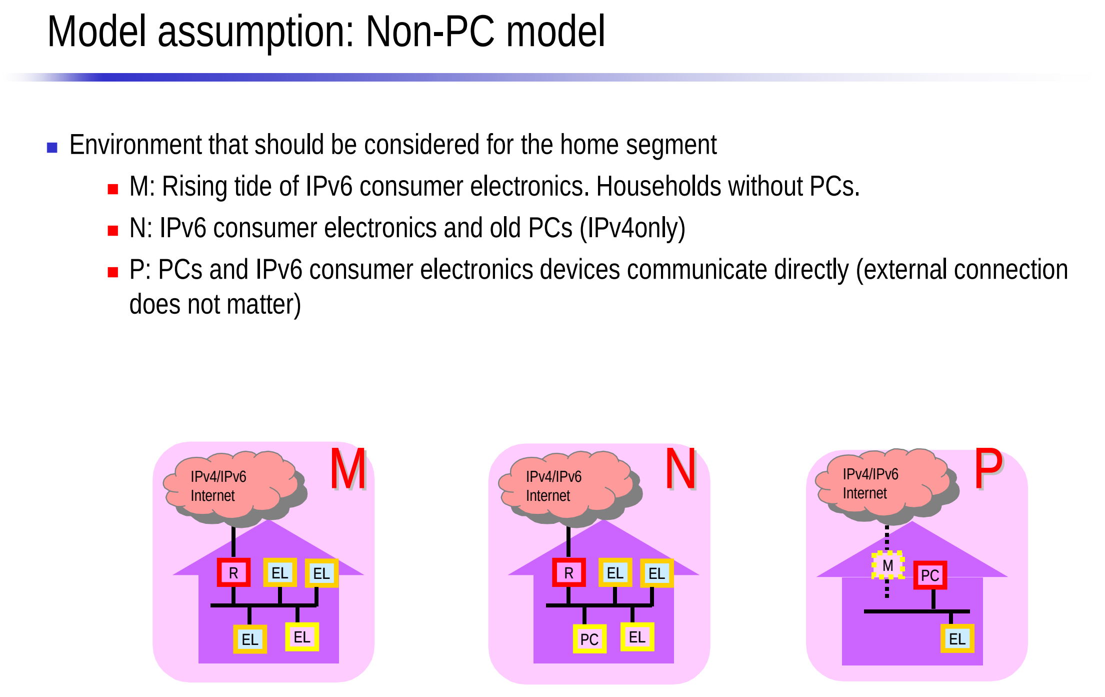
(Model L is basically the same as Models K.)

Model		L: Condition H + v6 devices remotely access devices in home
Description		Multiple PCs/devices in home, some PCs are dual, some are v6 only v6 external devices
Configuration	Boundary with network	Router (dual) connection
	Connected devices	PCs, game machines, non-PC devices (AV, consumer electronics, IP cameras, IP phones) v6 external devices (PC (PDA))
Applications used		Set VTR timed recordings from mobile phones, use external devices to view camera images inside the home.
Address	Internet side	/48/64prefix, DHCPv6, 6to4 auto generation, configured, DTCP
	Local side	Prefix is notified by RA, Link-local
Naming	Query	Same as H
	Registration	
Security measure	Encryption	Router, Windows XP (null coding IPsec)
	Measures to prevent unauthorized access	Packet filter by router. SPI Standard Windows XP support, v6 personal firewall is not yet implemented.
	Virus measures	Virus checker, use of services provided by ISP.
	DoS measures	No special measures
Setting method		Windows applications, unique setting method for each application, auto setting, update
Other		It is recommended that the translator function be implemented on the router. One point to consider is how to obtain a list of devices in the home.

Features of Model O

Model O is basically the same as Models K and L. However, with this model, the setting method and contents of non-PC devices become issues. Matters of concern are how to do naming and how to set devices to use DNS. For example, when there are multiple TVs and videos at home, how are they differentiated?

Model assumption: Non-PC model



Model assumption: Non-PC model

- Environment that should be considered for the home segment
  - M: Rising tide of IPv6 consumer electronics. Households without PCs.
  - N: IPv6 consumer electronics and old PCs (IPv4only)
  - P: PCs and IPv6 consumer electronics devices communicate directly (external connection does not matter)

In usage forms unique to the home segment, the following environments need to be considered.

M: Household with no PC in the first place begin to use IPv6 consumer electronics.
N: PCs use IPv4 but IPv6 consumer electronics are added.
P: PC and IPv6 consumer electronics directly communicate (external connection does not matter)

Features of Model M

Model		M: Extension of condition J
Description		Multiple devices at home; some are v4 only, some are v6 only Router (dual) is required.
Configuration	Boundary with network	Router (dual) connection
	Connected devices	Game machines, non-PC devices (AV, consumer electronics, IP cameras, IP phones)
Applications used		TV and video, use TV to view camera images inside home
Address	Internet side	/48/64prefix, DHCPv6, 6to4 auto generation, configured, DTCP
	Local side	Prefix is notified by RA, Link-local
Naming	Query	uPnP
	Registration	DNS server and naming method closed within home
Security measure	Encryption	Router. Handled by end devices.
	Measures to prevent unauthorized access	Packet filter by router. SPI No special measures for end devices (expect router to handle such matters)
	Virus measures	Service provided by ISP
	DoS measures	No special measures for end devices
Setting method		Since there is no PC, settings for routers and devices are performed using a browser such as a TV. (Depending on the browser, the setting screen may be unstable or not appear.)
Other		

The characteristics of Model N are basically the same as Model M but the existence of PC makes the following differences:

- Security measures can be implemented using a personal firewall on a PC.
- Possible to use a PC (browser) to set routers and other devices.

Features of Model P

Model		P: Island inside home model
Description		v6 consumer electronics and PCs are connected via a network at home.
Configuration	Boundary with network	No specific awareness
	Connected devices	V6 consumer electronics, PC (dual)
Applications used		Consumer electronics and PCs collaborate (timed video recording setting, recordings, video is copied to PCs and used, images are recorded with PC)
Address	Internet side	-
	Local side	Link-local
Naming	Query	uPnP, SLP, NIQ
	Registration	Performed each time equipment is used
Security measure	Encryption	No special measures. WEP, etc. when wireless technology is used.
	Measures to prevent unauthorized access	No special measures
	Virus measures	No special measures
	DoS measures	No special measures
Setting method		Settings are performed using browsers provided by such devices as a PC or TV. (Depending on the browser, the setting screen may be unstable or not appear.)
Other		

3.3.3 Points During Migration from Current Condition to BCP

Issues that need to be considered during migration from the current situation to BCP. Include:

Configuration

If possible, households having a dial-up environment should be encouraged to use routers.

Application

In the BCP stage, it is desirable to provide attractive IPv6 applications. When current applications remain, users are satisfied with IPv4. The Spread of IPv6-only IP phones may provide additional impetus. At the least, the current IPv4 applications are supposed to be continue to be used as is. In addition, there is a need to clear issues related to registration and use of addresses and names.

Security

It can be imagined that encryption (IPsec) will be performed at the router. For PCs, the emergence of personal firewalls that can handle IPv6 is expected.

Other

Establishment and automation of setting method for non-PC devices is expected.

3.3.4 Non-PC Deployment Scenario

When thinking about issues related to migration of non-PC devices to IPv6, basically, it is the same as the other general migration scenarios explained so far.

There are, however, two unique situations with non-PC devices that should be examined:

- In general, non-PC devices are not powerful and it is difficult to implement security functions. Therefore, we cannot help but rely on routers.
- Web browsers are the only option for configuring non-PC terminals or routers.

3.4 Issues on the Way to 50-50

3.4.1 Security

Unlike PCs, which are used based on the principle of self-responsibility, consumer electronics have a wider range of target users and usage methods. For that reason, with respect to security measures it is necessary to go a step further.

Encryption

There are three primary methods of encrypting communication data: (1) use of IPsec with routers, (2) handling by terminal devices and (3) individual handling at the application level. Encryption processing is technically possible through hardware processing but how keys are established and replaced are important issues. Can they be set up automatically? Will they have to be set up manually? If they are manually set up, service personnel will need to perform settings and so forth. We must choose a practical method.

Measures to prevent unauthorized access

If users register in a general external DNS, the risk of unauthorized access increases. Management of DNS information is a serious issue. To use IPv6, users at least need to have appropriate packet filtering via their home router. USAGI is gradually supporting stateful packet inspection on Linux. Since use of IPsec causes encrypted data to go through the router as is, terminal level handling of such data is necessary. Currently, no commercially available personal firewall products support IPv6. Windows XP includes support for an IPv6 personal firewall. Unlike PCs, however, many non-PC devices cannot protect themselves. Therefore, they must be protected by a router.

Virus measures

With regard to email software, since IPv4 supports it there is no need to go to IPv6 for the time being. About this matter, we will wait for the IPv6 support structure to become established. However, in the world of IPv6, there is a possibility that pattern files for virus software could be updated through a push type service (from the user’s point of view, forced updates of this type could sometimes be problematic).

DoS measures

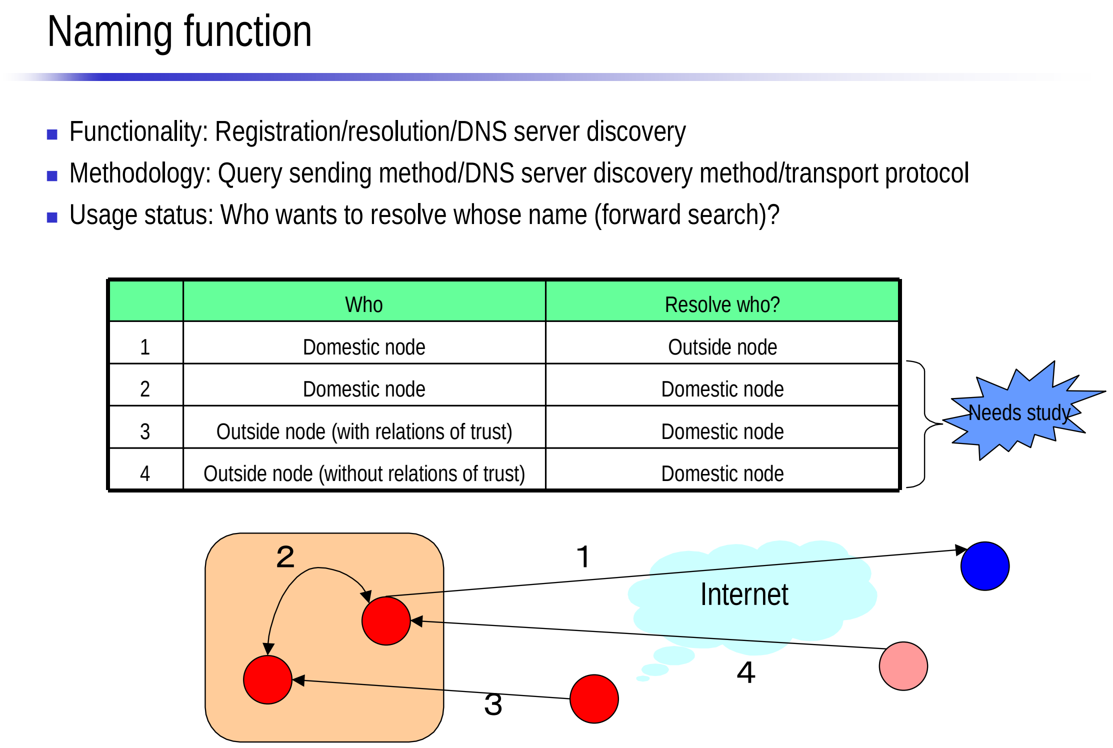
With regard to Denial of Service (DoS) attacks, there is basically no protection with either IPv4 and IPv6. It is possible to detect and block such attacks using an intrusion detection system. However, consumption of resources and decreased performance cannot be avoided. With an IPv4 stack, thanks to code improvement it no longer fails so easily under a DoS attack; however, there may be attacks that are unique to IPv6 stacks, though they are as yet unknown. ISPs are expected to take DoS attack countermeasures. Since we cannot expect non-PC devices themselves to include effective security measures, it is expected that the service side will deal with such issues.

3.4.2 Translator Function

Whether an IPv4-IPv6 translator function is needed depends on the need for collaboration between IPv6-only and IPv4-only devices. The location of such a translator function is thought to differ depending on the application.

It could be placed at an ISP or service provider outside the home or operate on routers. In that case, it is independent from the application and is thought to be the ideal style. Another possibility is that a translator is placed in the PC in the home. At the least, it is difficult to imagine how a special translator device would be installed in homes. Whatever the case, power of such function is expected to be ON all the time.

3.4.3 Naming Function



Naming function

- Functionality: Registration/resolution/DNS server discovery
- Methodology: Query sending method/DNS server discovery method/transport protocol
- Usage status: Who wants to resolve whose name (forward search)?

	Who	Resolve who?
1	Domestic node	Outside node
2	Domestic node	Domestic node
3	Outside node (with relations of trust)	Domestic node
4	Outside node (without relations of trust)	Domestic node

For naming, a function is needed in devices in the household to discover the DNS server, perform registration and resolve names. Issues include how to discover the DNS server, how to send a query and how to use transport protocols. In addition, it is necessary to clarify who resolves whose name (forward search). (For example, whether it should be made possible for any terminal in the household to determine the address of other terminals in the household.) The following section discusses issues and solutions for name resolution both inside and outside the household.

Name resolution in the household

The following issues can be expected in name resolution when a household device communicates with other devices in the same household.

1. DNS server discovery process
2. Query model
3. Registration of device information

DNS discovery process

To use the DNS system, terminals need to use some method to determine the DNS address. However, since there are devices in the home that do not have an interface to configure settings, this information must be set automatically. There are several automatic setting methods. If well-known Anycast or Multicast is used, security issues must be considered.

When a Unicast DNS server is used, it seems better to think about DNS information auto settings in the following order:

Router Advertisement → DHCP → Well-known Multicast → Manual entry

(The order of router advertisement and DHCP will probably be changed in future depending on implementation size and operation status).

Query model

With Multicast DNS, support is required at each node and the external query server is required. Since ICMP Node Information Query (NIQ) is not DNS, the program needs to be corrected. Anycast DNS and Multicast DNS face security issues.

The recommended method is the following order:

Unicast (auto setting) → Anycast (use of well-known address) → Multicast (no server) → Unicast (manual setting) → ICMP Node Information Query

Registration of device information

The method used in the home to register device information is to use FQDN or allow users to use any name they want.

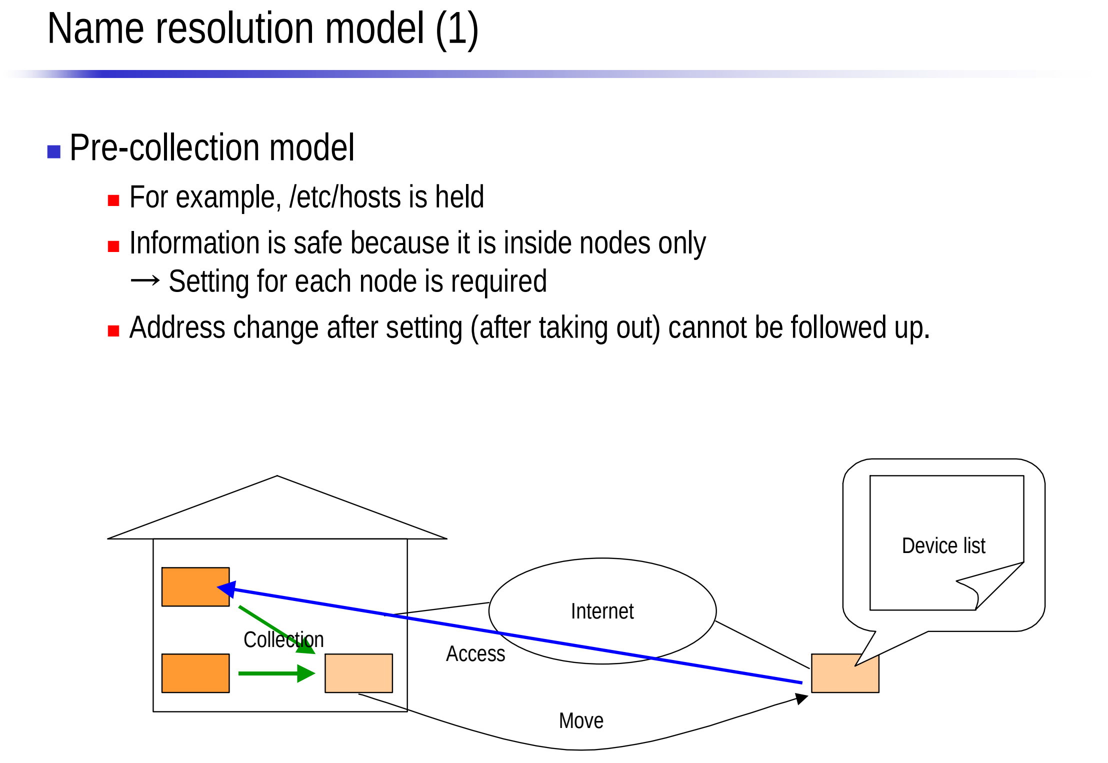
Name registration in the home, especially IP address input and registration, is very troublesome and some devices may not have even an interface for display or input. For that reason, auto registration means are essential, including DNS update, connection detection and auto registration.

In this case, certain issues must be solved, including, for example, to what extent information is opened, how to handle the privacy of individuals at home and how to assign names to differentiate devices when there is more than one of the same type of device in a home.

Name resolution from outside the household

When an outside note resolves a domestic node, the existing system of dynamic DNS or DNS Update can be used for registration but at which point the node should be registered is an issue. It should be carefully considered whether registration takes place at a server provided by ISP, a server provided by the device vendor or a third-party server. In addition, registered information and devices need to be decided. From a privacy protection point of view, the degree to which information is opened and the content of the information are very important issues.

Pre-collection model

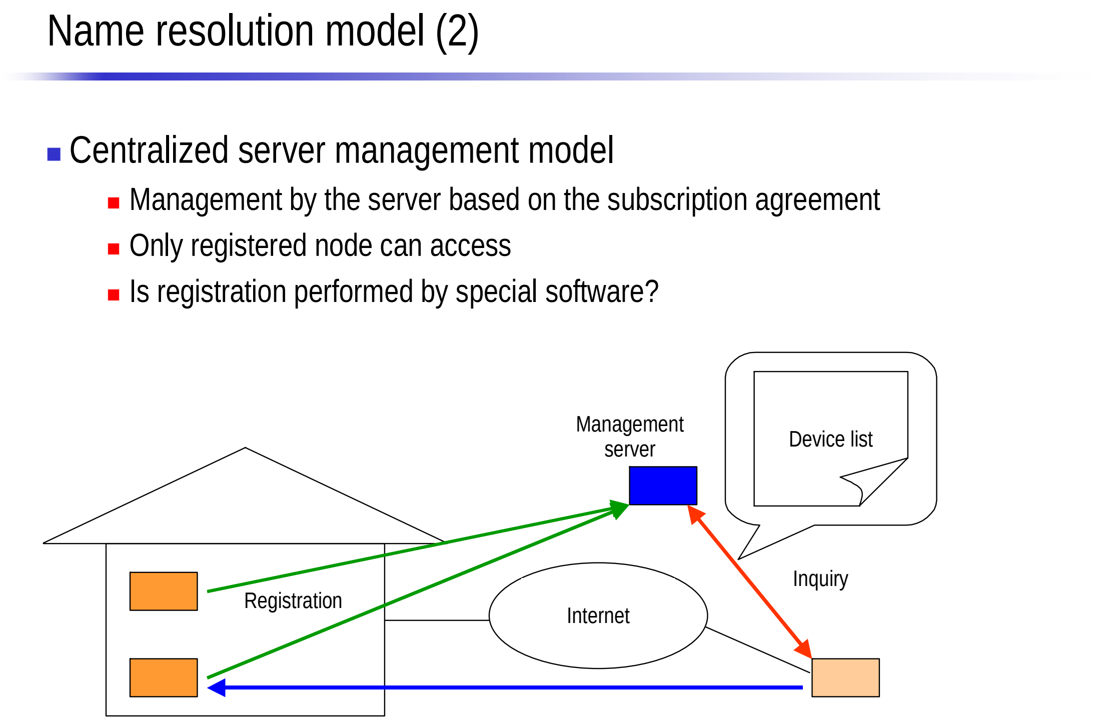


Name resolution model (1)

- Pre-collection model
  - For example, /etc/hosts is held
  - Information is safe because it is inside nodes only
    → Setting for each node is required
  - Address change after setting (after taking out) cannot be followed up.

With the pre-collection model, we can imagine a situation in which a device is carried out of and into a home obtains, for example, /etc/hosts information while it is inside the home, and while outside the home that information is used to resolve names. In such a case, the information only exists in the device that is carried out of home, thus it is secure. However, settings are required for each device. In addition, address change after setting (after taking the device out of the home) cannot be followed up.

Centralized server management model

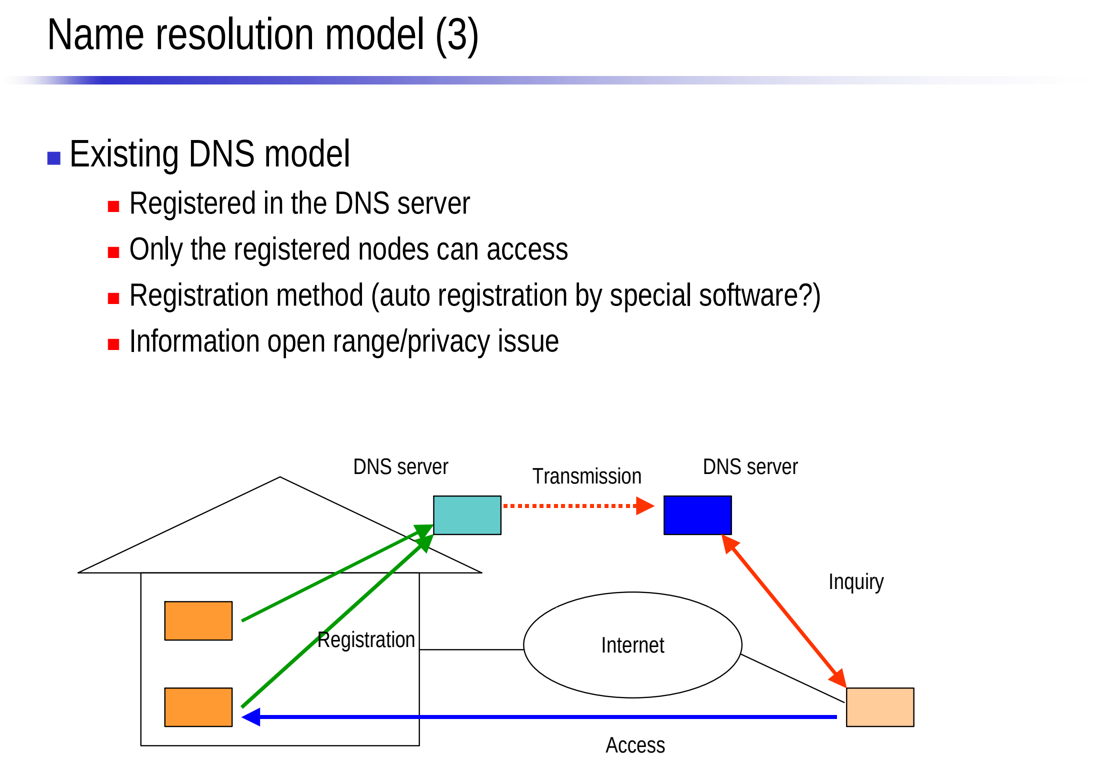


Name resolution model (2)

- Centralized server management model
  - Management by the server based on the subscription agreement
  - Only registered node can access
  - Is registration performed by special software?

In this case, based on some subscription agreement, a server placed on the Internet manages DNS information. This DNS server can only be accessed by registered nodes. Registration may be performed by special software.

Existing DNS model



Name resolution model (3)

- Existing DNS model
  - Registered in the DNS server
  - Only the registered nodes can access
  - Registration method (auto registration by special software?)
  - Information open range/privacy issue

With this model, nodes are registered in the existing DNS server and only registered nodes can access the server. There are two issues: (1) how to automate registration (the possibility of using special software) and (2) how to handle how open the information is and related privacy issues.

Other issues

Another issue is how to do with the transport protocol used related to DNS. In this regard, a dual stack is desired. The reason is that there should not be names that can only be resolved by IPv4 or IPv6. In addition, when you think of mounting a system with a home router, dual stack is no problem.

Another issue is the multiprefix environment. That is, with IPv6, it is possible that more than one network prefix is assigned to a terminal. However, as to how end nodes use these prefixes and how to select the source address for applications, clear answers have not yet been found.

In addition, to ensure security of communication related to DNS, DNSSEC has been discussed but there is no conclusion yet.

About automatic naming of non-PC devices, there is a remaining issue about how to differentiate devices when there is more than one device of the same type. In addition, when a list of names is displayed with an application, naming is expected to be easy for users to understand. Automation that addresses such matters is expected.

3.4.4 Connections to ISPs

In the BCP stage, there may be a case in which a device (or router) that wants to use IPv6 service uses a tunnel connection. There are various tunneling methods including static tunneling or dynamic tunneling such as DTCP, 6to4, ISATAP and Teredo. In BCP, the important thing is the type of connection but if possible we want to lead to a native or dual stack connection.

3.4.5 ISP Requests

Where there is a home router, there are various network configurations such as RA, DHCP, DTCP and ISATAP and the address grant method differs depending on the method. Whether the distributed network prefix is any of /48, /64 and /128 is a matter of concern as well. From the terminal vendor’s point of view, concerning migration of the home segment to IPv6, there is a request that the method to deliver addresses be identified.

For example, when /48 is used we can imagine a setting method in which a prefix is assigned for each translator, DMZ or QoS class.

In addition, when there is no home router, RA can be said to be desirable for information consumer electronics. There is a remaining issue in terms of security but there is also an advantage that additional implementation is not required.

3.5 Tips & Tricks

3.5.1 Overall Issues in the Home Segment

Version upgrade of software and firmware will likely frequently occur during migration from IPv4 to IPv6. It is necessary to have a method to perform upgrades as inexpensively as possible. For example, usually pull type methods are used but push methods are used when security problems occur. Such methods can be imagined.

How to support the mobile environment (when a device in a home moves to a hotspot outside the home) needs to be studied.

In addition, it can be assumed that some part of the non-IP devices (Echonet or IEEE 1394 devices) may shift to IP(v6) devices.

3.5.2 Non-PC Study Items

With non-PC devices, sufficient resources (CPU and memory) cannot be expected. For that reason, there are limitations on the functions that can be mounted. There is no room to mount both IPv4 and IPv6 stacks. When the OS is TRON, for which there may be no security functions or if there are only the minimum security functions are available (for example, when an IPsec or encryption chip is incorporated into hardware), it is necessary to confirm support for IPv6 stack and network system middleware (DNS, etc.). Also, though RA should be supported, we may expect router to take care of the remainder of those issues. Therefore, users must be encouraged to use routers.

Most non-PC devices have no method of setting or checking or at best have only a poor ability to do so. User ideas about consumer electronics at that they "just work” when connected. Even though there is a remote control, it cannot be said to be easy to use when there is just a couple-line LCD. Therefore, settings need to be automatic to the maximum extent possible. Service life of consumer electronics is long and there are issues such as how long single vendors will provide support, including provisioning of patches, etc.

3.5.3 Setting Methods Without PCs

Configuring settings without a PC is a big issue. When thinking about the spread of IPv6 among household devices, it cannot be assumed that PC will always be available. The same thing can be said for the IPv4 world. Therefore, it is expected that there will be a method to set up devices on an individual basis. We expect to be make auto settings available to the extent possible using zero-conf, etc. and also expect TV browser functions will be available (probably will be mounted). It may be possible to configure devices via a mobile phone browser or IrDA. It is assumed that the browser used will have a function that allows users to display a setting screen. If auto setting is not possible, a setting service must be provided separately.

4. IPv6 Deployment Guideline (SOHO segment)

4.1 Introduction

This document is intended for system integrators who engage in SOHO configuration and users and administrators who are studying deployment of systems and is intended to describe general items, guidelines and methods that should be considered with regard to use of IPv6 in SOHO environments.

The information in this document is intended not as a solution but to offer examples that readers can refer to for advice on specific management policies and constraints on the deployment of IPv6.

4.1.1 SWG Members

Chair
Inomata (Fujitsu Limited)

Members (in alphabetical order)
Arano (Intec NetCore, Inc.)
Kaneyama (Intec NetCore, Inc.)
Kato (Fujitsu Limited)
Kawashima (NEC Access Technica, Ltd.)
Kurose (Fujitsu Limited)
Nakai (NTT Communications Corporation)
Ozaki (Fujitsu Limited)

4.1.2 Inquiries

For questions related to Part 1, please send email to the following address:

IPv6 Promotion Council of Japan DP-WG

wg-dp-comment@v6pc.jp

4.2 Segment Features

4.2.1 SOHO Classification

Business offices called SOHO include the following:

1. **Family operations**
   Includes one PC and an Internet connection. This type of environment is similar to the home segment environment.

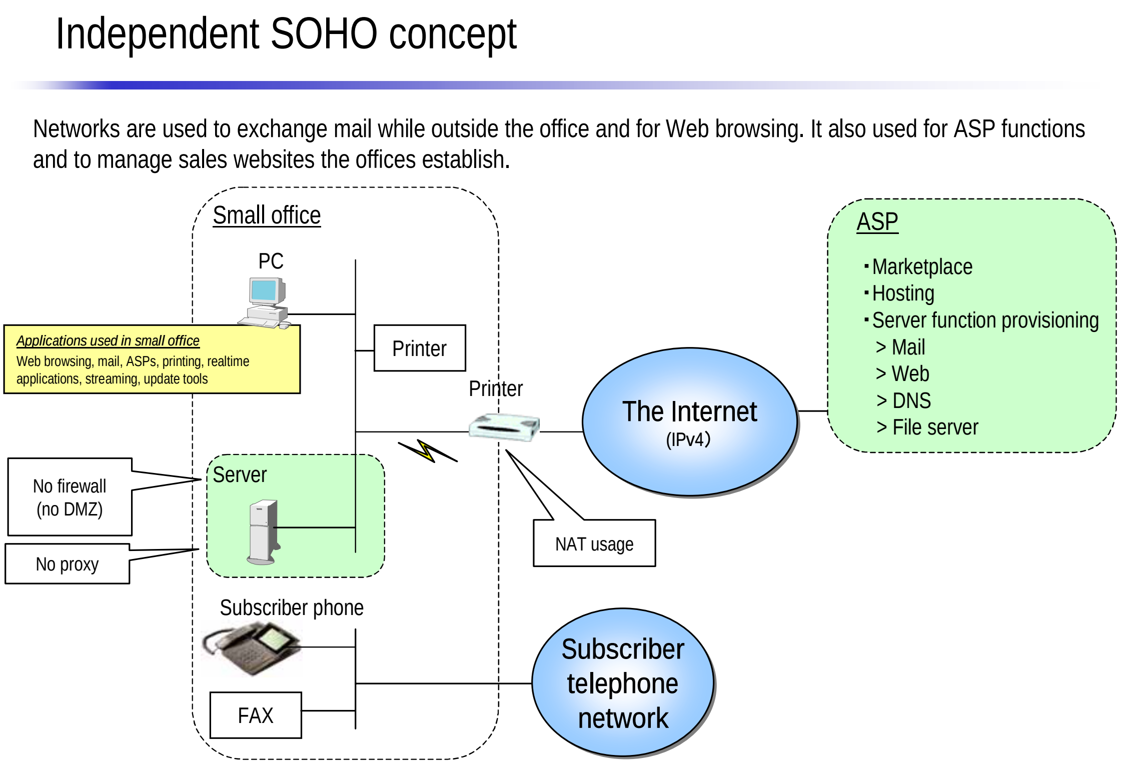
2. **Small business offices (independent SOHO)**
   Business that operates based on a single small basis. In addition to the components in item 1 above, the system is comprised of more than one PC and a single subnet LAN.

3. **Small sales offices (dependent SOHO)**
   A small office in a larger size organization. In addition to the components in item 2 above, the system is connected to an external network via VPN (headquarters, ASP center).

4. **Convenience stores**
   The system includes POS terminals and non-PC terminals. Many networks have a unique configuration.

In this deployment guideline, small business offices ("independent SOHO" environments) and small sales offices ("dependent SOHO" environments) are the subject of discussion.

4.2.2 Independent SOHO Concept



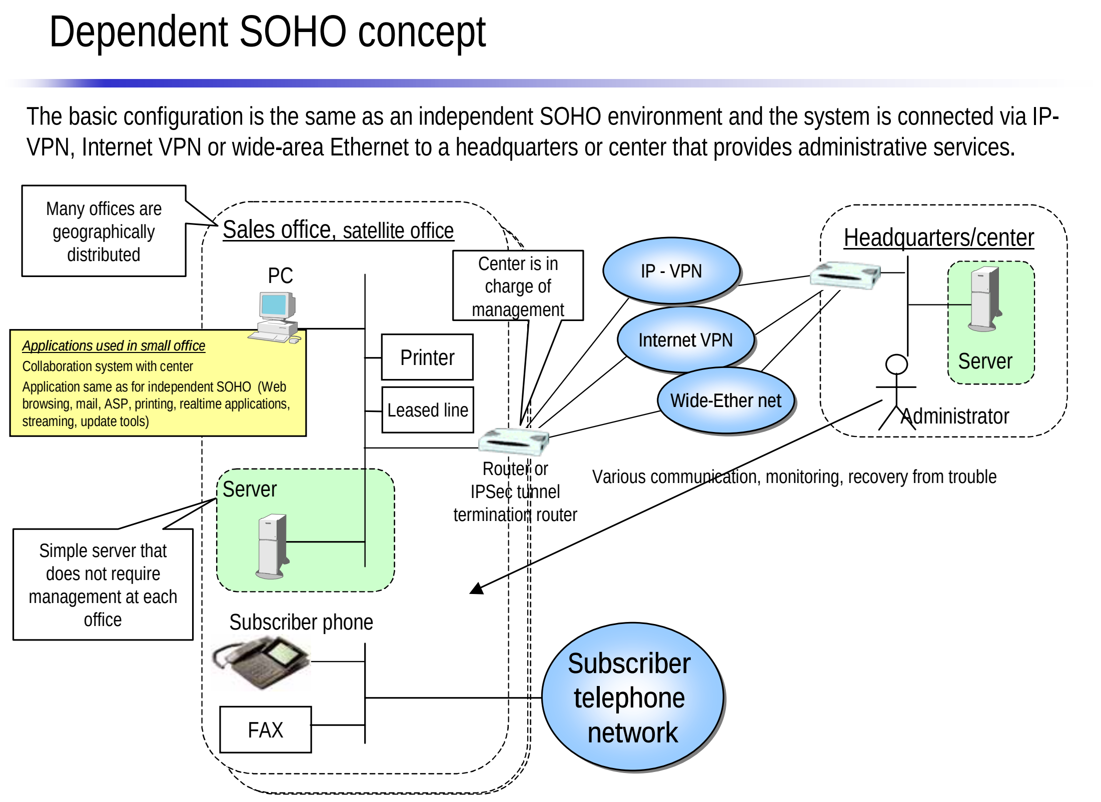
Independent SOHO concept

Networks are used to exchange mail while outside the office and for Web browsing. It also used for ASP functions and to manage sales websites the offices establish.

Small office
PC
Applications used in small office
Web browsing, mail, ASPs, printing, realtime applications, streaming, update tools
Printer
Printer
No firewall (no DMZ)
No proxy
Server
NAT usage
The Internet
(IPv4)
ASP
・Marketplace
・Hosting
・Server function provisioning
> Mail
> Web
> DNS
> File server
Subscriber phone
FAX
Subscriber telephone network

Networks are used to exchange mail while outside the office and for Web browsing. It is also used for ASP functions and to manage sales websites the offices establish.

4.2.3 Dependent SOHO Concept



Dependent SOHO concept

The basic configuration is the same as an independent SOHO environment and the system is connected via IP-VPN, Internet VPN or wide-area Ethernet to a headquarters or center that provides administrative services.

Many offices are geographically distributed
Sales office, satellite office
PC
Applications used in small office
Collaboration system with center
Application same as for independent SOHO (Web browsing, mail, ASP, printing, realtime applications, streaming, update tools)
Printer
Leased line
Center is in charge of management
Server
Simple server that does not require management at each office
Subscriber phone
FAX
Router or IPSec tunnel termination router
IP - VPN
Internet VPN
Wide-Ether net
Headquarters/center
Server
Administrator
Various communication, monitoring, recovery from trouble
Subscriber telephone network

The basic configuration is the same as an independent SOHO environment and the system is connected via IP-VPN, Internet VPN or wide-area Ethernet to a headquarters or center that provides administrative services.

4.3 Deployment Scenarios

4.3.1 Deployment Scenarios

This section describes the deployment phase by dividing into three steps: the current IPv4 usage phase, initial IPv6 deployment phase (IPv6:IPv4 = 1:9) and full-scale IPv6 deployment phase (IPv6:IPv4 = 50:50).

Two scenarios in the initial deployment phase

In the IPv6 initial deployment phase, two scenarios can be expected, depending on the purpose of deployment.

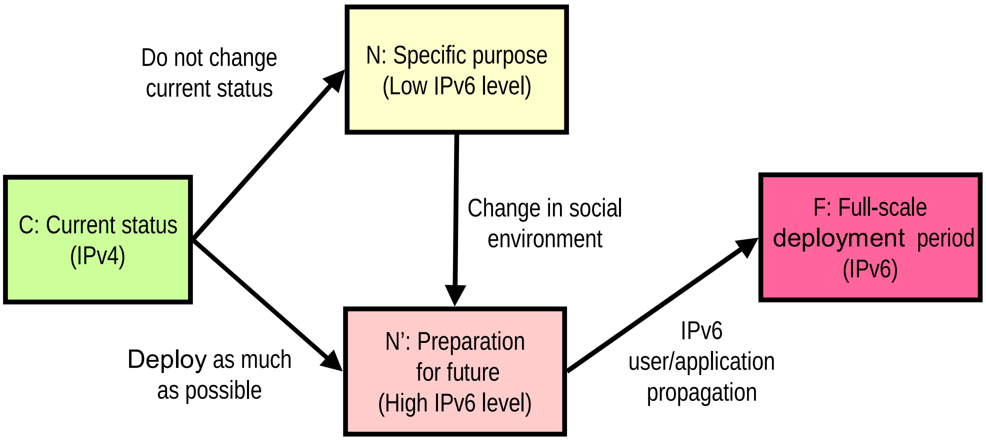
① Deployment for a specific purpose
In this case, IPv6 is deployed for some business purpose. This is triggered by certain factors, for example, when an application such as IP phone or instant messaging begins to use IPv6, or when business partners migrate to IPv6 to reinforce security for business transactions or maintenance purposes. This scenario basically does not change the IPv4 network and can be considered to be a conservative IPv6 deployment scenario.

② Deployment to prepare for future
This scenario assumes that IPv6 will be widely adopted in future and prepares to use IPv6 when the system is replaced. This can be said to be active IPv6 deployment.

Part 1 assumes that the current IPv4 usage changes in two ways, one is when IPv6 is deployed for a specific purpose and the other is when IPv6 is deployed in preparation for future activities. Furthermore, IPv6 deployment based on specific purpose evolves into active IPv6 deployment for the future and a full-scale deployment phase begins.

Relationship between scenarios

Relationship between scenarios



C: Current status (IPv4)

Do not change current status

N: Specific purpose (Low IPv6 level)

Deploy as much as possible

N': Preparation for future (High IPv6 level)

Change in social environment

IPv6 user/application propagation

F: Full-scale deployment period (IPv6)

Classification	C: Current	N: Next	N': Next'	F: Future
Time	Now	One year later	One year later	2-4 years
Network content	Before deployment	Simple IPv6 deployment	Full-scale IPv6 deployment	Complete IPv6 deployment
IPv4/IPv6 communication	IPv4 only	Tunneling, translator	Dual stack	IPv6 native

The above illustration shows the flow from the current situation (C) to the full-scale IPv6 deployment phase (F) including the two scenarios discussed above. Specific purpose (N) preparation for future (N') is assumed to be in one year and the full-scale deployment phase (F) is in two to four years.

4.3.2 Focus of Study

The following items are discussed in Part 1:

① Network

Classification of communication terminals

- Terminals that only communicate inside LAN.
- Terminals that communicate both inside LAN and with the Internet
- Terminals that only communicate with the Internet (Example: A telephone without an extension function)

Type of links used

IP address (distribution, setting, communication)

② Application

- Information-related communication: Web browsing, mail, ASP
- Real time communication: Printing, VoIP, streaming
- Management-related application: UPnP, update tool

③ Security

- Network security
- Terminal security

4.4 Independent SOHO Migration

4.4.1 Overview of Independent SOHO Configuration

Assumptions about independent SOHOs

We assume small offices of independent businesses to be examples of independent SOHO operations. Typical examples are accountant and design offices that have about 10 staff and, generally speaking, not particular high level of IT skill. In some cases, there are a couple of people that are familiar with IT.

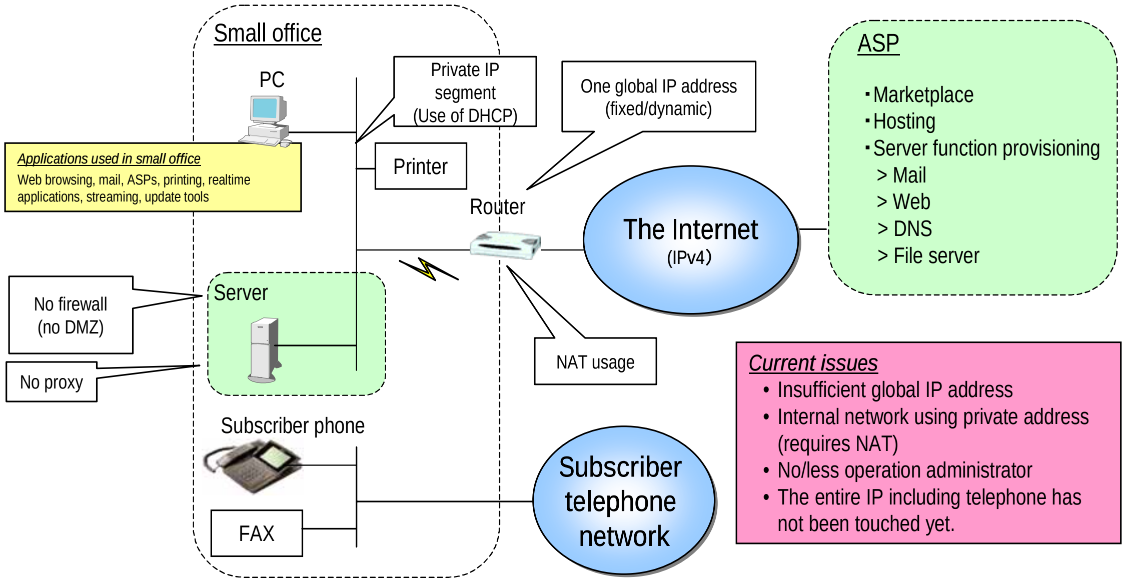
The office is in one location and staff travel to various locations. Staff communicate with personnel in other companies, staff on business trips and employee family members. Because the business is small scale, there is little budget for networking and they usually do not have complicated servers.

Terminals placed in independent SOHO operations are mostly PCs and sometimes file servers. Such offices also have printers, telephones and FAX machines.

Independent SOHO concept

Independent SOHO concept

Networks are used to exchange mail while outside the office and for Web browsing. It also used for ASP functions and to manage sales websites the offices establish.



Small office

PC

Private IP segment (Use of DHCP)

Printer

One global IP address (fixed/dynamic)

Router

The Internet (IPv4)

Applications used in small office

Web browsing, mail, ASPs, printing, realtime applications, streaming, update tools

No firewall (no DMZ)

No proxy

Server

NAT usage

Subscriber phone

FAX

Subscriber telephone network

ASP

- Marketplace
- Hosting
- Server function provisioning
  - > Mail
  - > Web
  - > DNS
  - > File server

Current issues

- Insufficient global IP address
- Internal network using private address (requires NAT)
- No/less operation administrator
- The entire IP including telephone has not been touched yet.

Networks are used to exchange mail while outside the office and for Web browsing. It is also used for ASP functions and to manage sales websites the offices establish.

4.4.2 Migration of Network to IPv6

Migration of network

① **Use of IP address**

Analysis

Terminals in a LAN will acquire a link-local address for an IP address when IPv6 is deployed. In addition, if a global address can be granted to the LAN, communication with the global environment is possible. Based on addressing policies, global prefixes (dynamic/fixed) provided to LANs use /48 or /64. Multiple patterns (/64 to /48) of prefixes distributed inside the LAN can be expected.

Since at this stage a source address selection function is not implemented in applications, it is necessary to try various measures for communication using multiple prefixes.

In addition, in offices of this size, multiple segments make communication management such as printer connections or file sharing complicated. Therefore, generally a one segment configuration is used.

In the near term

For the above reason, currently during IPv6 communication the link-local address and global IPv6 address are used. This is advantageous in terms of P2P communication. It seems that of the available global prefixes, /64 is generally used. Since the configuration is one segment for the time being, it does not seem that an additional prefix will be necessary.

Issues

We need to study how to handle addressing when a /64*n global prefix is used in future.

② **DNS related issues**

Analysis

With regard to the auto DNS setting function of IPv6, it is not implemented in Windows OS, etc. However, it is possible to reference IPv6 host information using the IPv4 DNS. For some broadband routers, proxy DNS query has already been implemented.

In the near term

Therefore, it seems reasonable to share the IPv4 DNS and have the router perform DNS querying to handle IPv6 name resolution.

Issues

However, IPv6-based methods are becoming standardized (Well Known Address, DHCPv6, etc.) and it seems this issue will be resolved in future.

③ Link form

Analysis

For connection with ISP, two services are provided, a tunnel connection and a native connection.

In the near term

It is OK to select a tunnel connection when the existing environment is used as is but this requires complicated router settings. In addition, many tunnel connections do not support automatic setting of network addresses. On the other hand, auto address assignment is supported by the ADSL native connection service used in SOHO environments. We recommend the native connection if simple settings are desired.

Devices required for network migration

Devices required for network migration of independent SOHO are as follows.

PC and server using an OS that supports IPv6

The latest versions of all the most commonly used operating systems already support IPv6 (Windows XP, MacOS, Solaris, Linux, etc.).

Broadband router support for IPv6

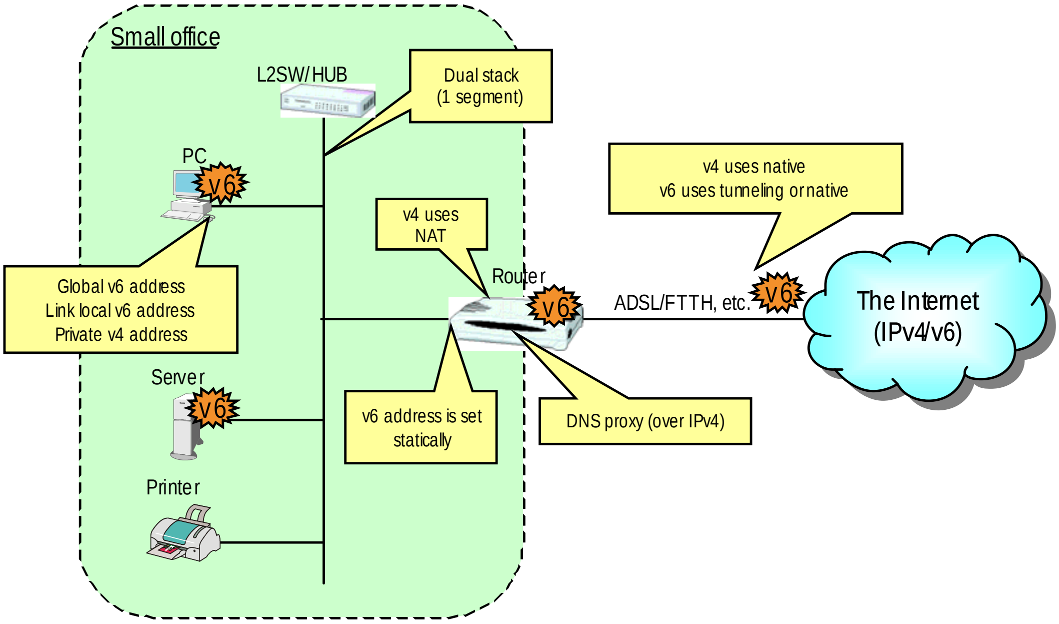
As a required function for IPv6, Router Discovery is supported and also the DHCP Prefix Delegation mechanism may be used by some ISPs, thus it is necessary to implement this mechanism. Furthermore, when using the tunnel connection, an IPv6 over IPv4 tunnel function is expected. Currently, IPv4 functionality is essential as well.

LAN switch/hub

If the layer 3 switch function is not used, currently available products are sufficient. However, even if only the layer 2 switch function is used, some switches check the type value and do not pass a type other than IPv4. It may be necessary to check the switch if it is old.

Network concept in near term / limited deployment case

Network concept in near term / limited deployment case



Small office

L2SW/HUB

Dual stack
(1 segment)

PC

v6

v4 uses native
v6 uses tunneling or native

v4 uses
NAT

Router

v6

ADSL/FTTH, etc.

v6

The Internet
(IPv4/v6)

Global v6 address
Link local v6 address
Private v4 address

Server

v6

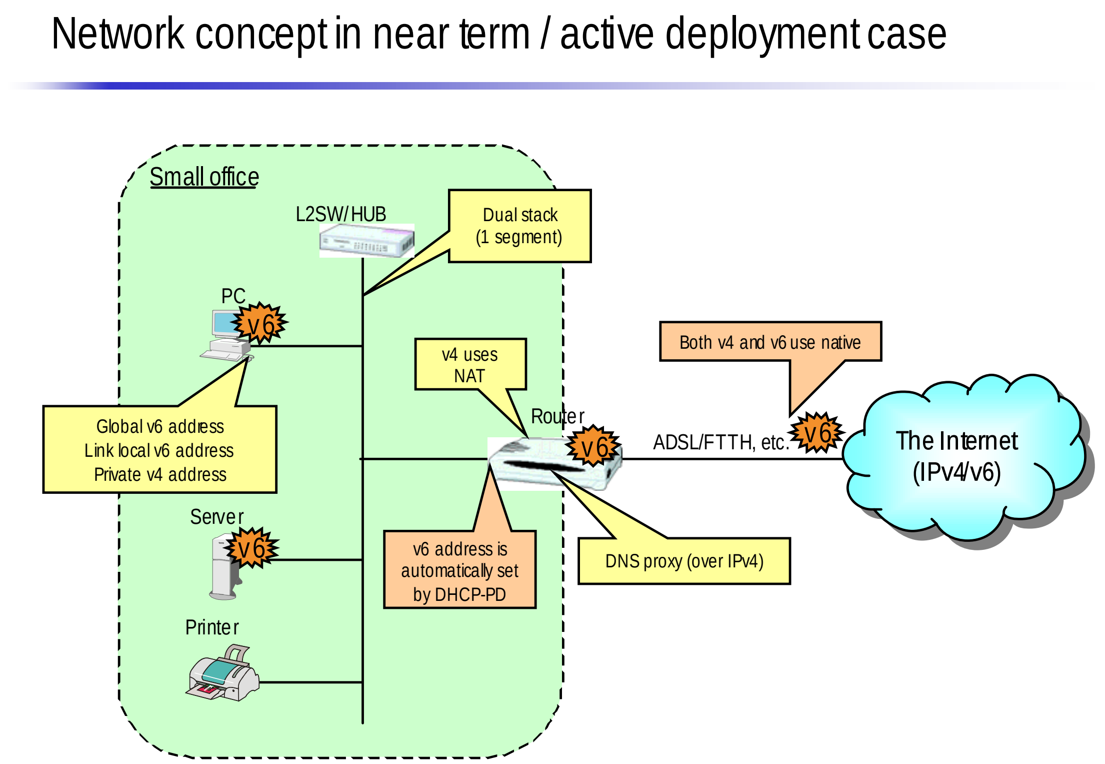
v6 address is set
statically

DNS proxy (over IPv4)

Printer

In the near term, networks for specific purpose deployment (limited deployment) are as shown above. For connection with an ISP, either a dual stack connection service with IPv4 is used or tunneling of IPv6 on the IPv4 connection service is used. IPv6 network prefixes are set statically in the router.

Network concept in near term / active deployment case



Network concept in near term / active deployment case

In an active deployment, an IPv4/IPv6 dual connection service is used. The IPv6 network prefix is automatically set in the router using DHCP-PD.

Summary

It seems OK for the time being for one /64 global prefix to be assigned for the IP address used by an independent SOHO. Depending on the application for which the network is used or if ISP service diversifies, use of multiple network prefixes may become necessary.

For connection with an ISP, a tunnel or native connection is selected depending on need. With regard to the DNS, IPv6 address resolution is performed by IPv4 transport for the time being. About this matter, it is efficient to use the IPv4 DNS proxy function of broadband routers.

4.4.3 Migration of Applications to IPv6

Current analysis of applications

With an independent SOHO, the server for usual applications (mail, DNS, WWW, etc.) is configured in the LAN or provided by an external network. Sometimes an ASP or marketplace is used. As a mechanism to supplement communication between a private address and external network, UPnP is used in some cases (communication tools, etc.)

PKI collaboration and Remote Access Service (RAS) are not used so much and in general certification is handled through server certification on a browser. However, in future it is expected that client side certification collaboration using USB tokens, etc. will increase. With an independent SOHO, applications (file sharing, printing, etc.) operating on a closed LAN are used.

Migration of applications

① Web browsing

Analysis

About migration of Web browsing, many browsers including Microsoft Internet Explorer support IPv6. On the server side, many Web server software applications such as IIS and Apache also support IPv6. For that reason, in terms of simple browsing, they can be used with the same effectiveness as IPv4.

With regard to security, however, virus check software such as Norton or Trend Micro does not support IPv6. Also, privacy issues can be pointed out, such as recognition of originating IP address information by a Web server a user is communicating with.

In a dual stack environment, consistency with IPv4 is ensured. If an IPv6 single stack is used in future, a proxy or translator becomes necessary and such devices are installed either at the ISP or within the site.

In the near term

In any event, it is hard to imagine that IPv6 deployment at the Web server side will progress rapidly and it seems likely that a dual stack environment will be essential for the time being. As to security, it is safe to perform usual browsing with IPv4.

Issues

A translator or reverse proxy is required to browse an IPv4 website from an IPv6-only device or environment.

② Mail (between mail client and server)

Analysis

Use of client-server type IPv6 mail is not different from IPv4 mail. The difference from the Web is that the mailbox (accessed point) only exists at a location to which the user subscribes. For that reason, if the ISP you use begins supporting IPv6, IPv6 support is easy. However, very few mail client software applications currently support IPv6. For that reason, virus checking software such as Norton or Trend Micro does not support IPv6.

In terms of mail, points that must be considered when migrating from a dual stack environment to an IPv6-only environment are the possibility of increased amounts of SPAM and the risk that mail from specific addresses will not arrive. Furthermore, association lists (like third-party relay lists) between IPv4 and IPv6 may also be used.

In the near term

With regard to security, even when a mail client supports IPv6, if virus checking software does not support IPv6, it is reasonable to prohibit IPv6. Mail is a client-server model that functions in the same way as Web browsing, thus there is less advantage to move to IPv6 and use of only IPv4 does not affect IPv6 migration overall. Even though the move to IPv6 is put off for now, it might be OK to do so later by monitoring the shift to IPv6 by other applications.

In future, in addition to the client-server type mail model, a P2P mail model may begin to be used as well.

Issues

IPv6 support by security checking software is an issue.

③ ASP

Analysis

ASP services for SOHO environments include e-commerce, groupware and business-specific applications. Unlike large enterprises, in SOHO environments the need for front office-related services such as information services is greater than back office-related services such as ERP. From a protocol point of view, services can be classified as Web-based ASPs or proprietary protocol ASPs (communication tools other than the Web, such as Lotus Notes, etc.).

In the near term

For Web-based ASPs, taking the same action as for Web browsing is reasonable. About proprietary protocol ASPs, it may become possible to migrate to IPv6 when large numbers of software applications begin to provide IPv6 support.

Issues

Some ASPs who use proprietary protocols may need to modify applications.

④ Printing

Analysis

There are currently no commercially available printers that directly connect to networks and support IPv6. However, it is possible to connect a terminal (server) that supports IPv6 to a printer.

In the near term

In the near term, IPv6 deployment policy is such that local printing is possible even when a printer does not support IPv6. However, to satisfy the needs for remote printing, support for IPv6 is expected.

Like products such as consumer printers that only support USB or IEEE1394 connections, there is a possibility that IP will be supported in those protocols in future. In that case, whether both IPv4 and IPv6 or only IPv6 will be used is unknown. There is a possibility that Windows IPP will support IPv6.

Issues

About use of IPv6 with printers, in addition to printing functions that support IPv6, there are latent needs such as the ability to perform diagnostic checks on printer devices and perform remote maintenance to check consumable status. There is already a health check service for FAX machines that is performed via telephone lines. When such services are used, the printer and service server automatically communicate, thus the service provider and user companies need to set up rules that govern how communication packets are transmitted.

⑤ P2P applications (VoIP, etc.)

Analysis

Support for IPv6 during P2P communication is possible if the application supports IPv6. Since communication is easily affected by NAT and there may be reluctance to adopt flexible communication, IPv6 may hold certain advantages in this area. For example, as opposed to IPv4 implementations, IPv6 IP phones do not need SIP-NAT, thus it is easier to deploy IPv6.

With regard to SIP, SIP servers are basically essential with IPv4. On the other hand, with IPv6 it is possible to directly communicate without the need for a SIP server. To ensure connectivity to an unspecified number, a phonebook function (a database function like LDAP) is required. If a VoIP gateway has this function, communication with specific parties is possible. A function to add phonebook entries is also a useful feature for a VoIP gateway phonebook function.

A communication packet translator must be installed to connect IPv4 and IPv6 IP phones. In terms of cost and management, use of such servers may be a bottleneck in the migration to IPv6. Translators that can easily be installed at SOHO sites and ISP-provided translator services are expected.

In the near term

In the near term, with regard to migration of P2P communication centered on VoIP, if the application supports IPv6 and also the other party supports IPv6, it seems OK to actively use it. Also, introduction of serverless P2P communication should be studied.

Issues

A highly scalable security protection mechanism that can be used with large-scale systems is expected. A highly scalable mechanism is required for connections between IPv6 IP phones and IPv4 IP phones.

⑥ **Video streaming**

Analysis

Use of video streaming in SOHO environments is not so popular with IPv4 because, for one thing, less content is being sent than received, and, in the near term, inbound usage is the primary focus. However, with respect to migration to IPv6, Windows Media Player already supports IPv6 and in technological terms use of video streaming is no problem.

In the near term

With IPv6, since it is possible to realize an environment where multicasting can be easily performed, the move to IPv6 is advantageous in terms of streaming. If attractive IPv6 broadcasting stations are available, support for IPv6 is worth studying.

⑦ **Update tool**

Analysis

There are two methods of performing updates from a management center, pull type updating and push type updating. When IPv6 is supported, secure control of individual terminals is possible and push type updates are easy to perform. Primary functions include a control terminal search, multicasting and non-PC control. The client-server model is used for update tools for independent SOHO environments.

In the near term

For general update services (Windows update, virus pattern file updates, etc.), it seems that IPv4 will only continue being provided for the time being. However, with special applications such as business applications, update tools and servers are custom-tailored. For that reason, IPv6 support can be realized relatively consistently. We can also study changing to a push type model in which IPv6 characteristics can be utilized.

Clients necessary to migrate applications

Typical clients that can be used with IPv6 include:

Web browsers	:	Microsoft Internet Explorer, Mozilla, etc.
Mail software	:	Win Biff, Edmax

Video streaming	:	Windows Media Player 9
IP phones	:	Some software phone applications support IPv6. Hardware phones include those produced by IWATSU ELECTRIC CO., LTD.

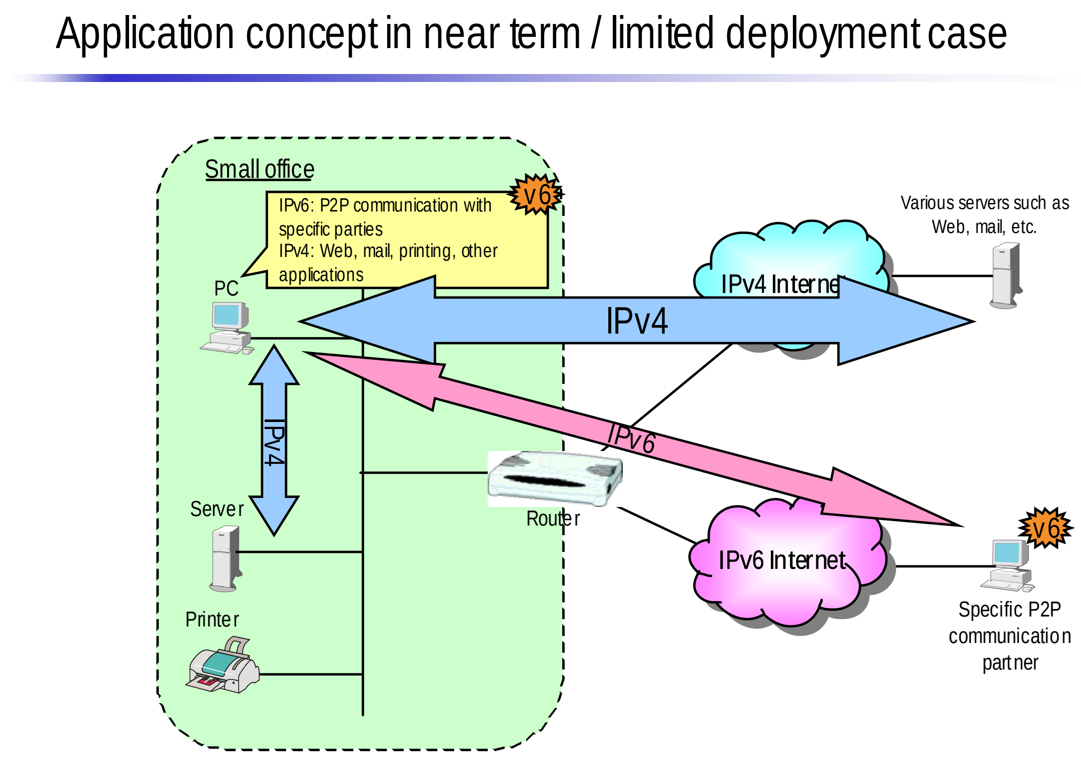
Applications that take advantage of IPv6 support include real-time (P2P) and streaming applications. With IPv6, one significant advantage is that NAT is not required.

A point of some concern is that, for reasons related to use of the Web and the DNS system, the current IPv4 network is also required. We believe applications that support IPv6 should be selected according to purpose. It is also necessary to confirm whether servers or subscribed services support IPv6.

Summary

The promise of P2P communication with specific parties is worth the move to IPv6. Since NAT is not required, the cost for address port management can be reduced and it is good for performance (delay, throughput) as well. There are less advantages to migrate current IPv4 applications such as Web browsing and email to IPv6 and the move to IPv6 there is also a higher risk in terms of security.

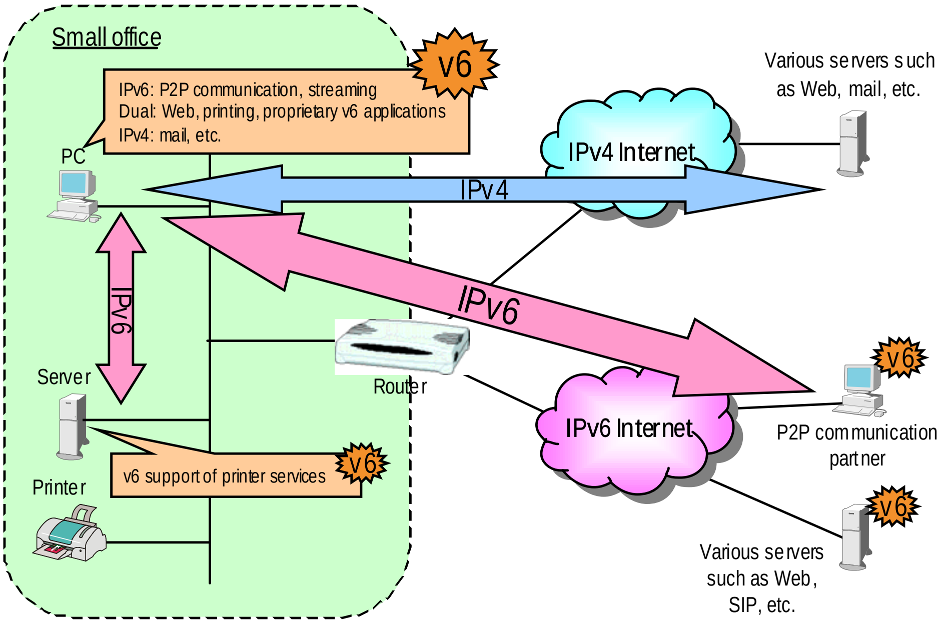
Application concept in near term / limited deployment case


Application concept in near term / limited deployment case
Small office
v6
IPv6: P2P communication with specific parties
IPv4: Web, mail, printing, other applications
PC
IPv4
IPv6
IPv4
Server
Printer
Router
Various servers such as Web, mail, etc.
IPv4 Interne
IPv6 Internet
v6
Specific P2P communication partner

In a limited deployment scenario, IPv4 is used for Web applications, email and printing and IPv6 is only used for P2P communication with specific parties.

Application concept in near term / active deployment case

Application concept in near term / active deployment case



Small office
v6
IPv6: P2P communication, streaming
Dual: Web, printing, proprietary v6 applications
IPv4: mail, etc.
PC
IPv4
IPv4 Internet
Various servers such as Web, mail, etc.
IPv6
IPv6
Server
Router
v6 support of printer services
v6
Printer
IPv6 Internet
v6
P2P communication partner
v6
Various servers such as Web, SIP, etc.

In an active deployment scenario, P2P communication and streaming are migrated to IPv6, while Web and printing use the dual protocol and proprietary applications use IPv6 as well. Email continues to use IPv4.

4.4.4 Migration of Security Management

Gateway security

Analysis

- **Encryption**
  Encryption for communication is necessary for telephone/fax, remote access by employees, business outsourcing and remote maintenance. Direct IPsec communication is performed between terminals, and devices such as sensors, etc. perform IPsec communication via a gateway. In this case, settings are required to keep devices in the communication path from hindering encrypted communication.

- **Measures to prevent unauthorized access**
  When implementing E2E communication with IPv6, unlike UPnP, IPv6 does not require a mechanism to open a port by itself. Therefore, there is no need to be concerned about security holes that are related to the port opening mechanism. However, when terminals in a office are registered in an open DNS, they may be the subject of certain kinds of attacks. Therefore, protection by filtering becomes necessary. Stateful packet inspection is performed and traffic is controlled on a terminal or port basis. Windows XP includes a personal firewall that includes IPv6 support thus use of this firewall is another option.

- **Virus measures**
  Simple IDS is used. In this case, attack pattern files are retained in the firmware and automatic update of both firmware and attack patterns is desired. Until virus check products begin to provide IPv6 support, we recommend that use of mail be prohibited with IPv6.

- **DoS attack measures**
  With IPv6, reachability from outside by NAT can be improved but each terminal is vulnerable to a DoS attack. As a measure for this, IDS needs to support IPv6.

- **Firewall**
  With regard to firewalls, as with IPv4, stateful packet inspection is used.

In the near term

With regard to gateway security, even if IPv6 is introduced, other than P2P communication the model is the same as with IPv4. Stateful packet inspection is used for firewalls. When performing P2P communication, it seems better to limit communication in which the address of the parties can be identified and in which ports are opened.

Issues

One issue is difficulty configuring security policy settings for P2P communication-related use. It is expected that a means will be provided by which users without special knowledge can correctly configure addresses and other settings.

Terminal security

Analysis

To safely perform P2P communication, it is expected to enable IPsec communication termination at terminals. However, when open DNS registration is used, if the host address of terminals is opened, there is a risk that the level of security will fall.

With regard to terminal security related matters, the elements of IPv6 that have not progressed sufficiently include packet filtering (personal firewall, etc.) for hosts, IDS and virus checking. In addition, with regard to virus measures, IPv6 support is expected with respect to function updating via pattern push from centers. About the Windows standard PKI function, IPv6 support in ESP (encryption, etc.) is expected.

On the other hand, functions that can be used as is on the IPv6 network include application level check (file infection check, etc.), use of IDs/passwords, server certification retention by browsers, and use of PKI or IPsec by special clients.

In the near term

A model similar to IPv4 can be used. Use of only IDs/passwords and use of Web server certification is no problem. For P2P communication, at the moment is seems best for this to be handled through gateways. Some products ensure security at the terminal level.

Issues

It is expected that virus checkers and personal firewall products will provide IPv6 support. In addition, it is expected that there will be common ideas about how to ensure security at the terminal level. For that reason, configuration of such tools needs to be simple.

Summary

With regard to IPv6 migration of independent SOHO environments, the following security issues need to be addressed.

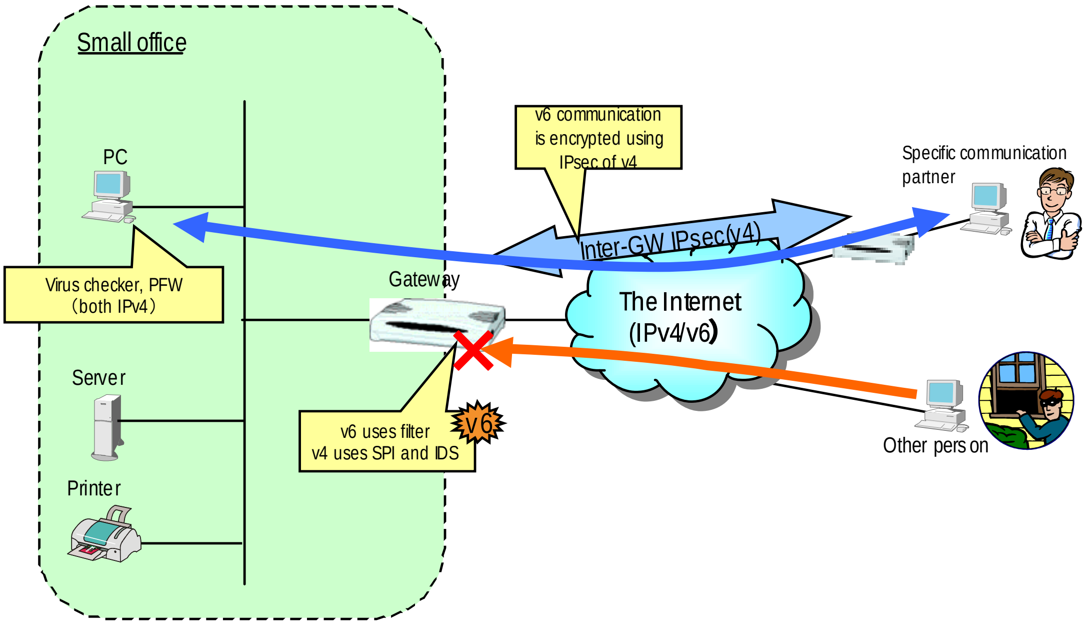
About encryption, first of all, the IPsec tunnel mode function built into some routers and encryption using a special client are used. SSL level encryption is valid with IPv6 as well.

With regard to measures to prevent unauthorized access and DoS attacks, stateful packet inspection is used for normal client-server type communication and filter-based security is used for P2P communication. Filter-based security is effective when the communication partner (address) is fixed. To the extent possible, terminal addresses on a network should not be registered in the open DNS.

With regard to terminal security, application level tools (virus checking of files, etc.) are valid with IPv6 and can continue be used. Some personal security tools (mail virus checking tool, etc.) do not operate with IPv6, thus it is better if applications do not support IPv6 if there is no reason to do so. In addition to terminals, because it is easy to configure security settings that collaborate with a gateway, we recommend that both terminal and gateway filters be used.

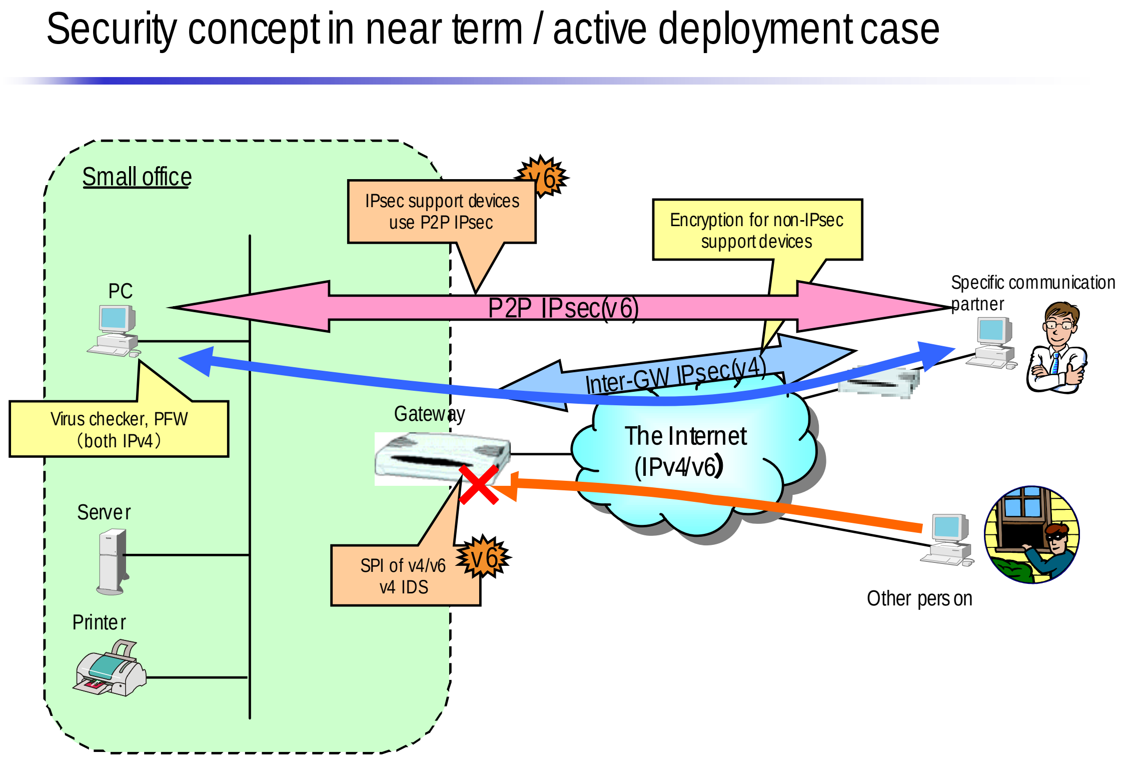
Security concept in near term / limited deployment case

Security concept in near term / limited deployment case



In the limited deployment scenario, encrypted communication with specific parties is performed using IPsec between gateways via the IPsec function of routers, etc. If encryption is desired for IPv6 communication, encryption on IPv4 is performed. If communication with other parties is needed, holes are punched in the router for that purpose. Boundary security related to IPv6 is handled through filtering.

Security concept in near term / active deployment case



Security concept in near term / active deployment case

In the active deployment scenario, communication with specific parties can be protected using IPsec between gateways and peer-to-peer encryption is used for IPv6 devices that support IPsec. For communication with other parties, a stateful packet inspection firewall that supports IPv6 is used.

4.4.5 Independent SOHO Migration Summary

With regard to migration of independent SOHO environments to IPv6, network migration, application migration and security migration are summarized below.

Summary of network migration

Item	C: Current	N: Next	N': Next'	F: Future	Issues
Link used	PPP etc.	Tunnel from router or terminal	Native	Native	Multi-Link Subnet Router (MSR)
LAN address	Private address	Dual Stack Single /64	Dual Stack Single /64	IPv6 only Multiple /64	Management when multiple prefixes are used
IP address distribution from ISP to user	PPP etc.	Static	Auto allocation (DHCP PD is used)	Auto allocation (DHCP PD is used)	
IP address distribution to LAN communication terminal	DHCP	RS/RA	RS/RA	RS/RA or DHCP (?)	
Setting of DNS to LAN communication terminal	DHCP	IPv4 is used (DNS query proxy)		IPv6 support in DHCP or Well-Known Address (?)	Standardize

Summary of applications migration

Item	C: Current	N: Next	N': Next'	F: Future	Issues
Web browsing (including ASP web base)	IPv4 access	IPv4 access special server will support IPv6	Dual Stack access	IPv6 access + Translator	Security check tool
Mail	IPv4 access	IPv4 access	IPv4 access (client server), IPv6 access (P2P)	IPv6 access (client server, P2P)	Security check tool (especially viruses)
Proprietary application	IPv4 access	IPv4 access (Note)	Dual Stack access? (Note)	IPv6 access? (Note)	Note: Maker dependent
Printing (including file sharing)	IPv4 access	IPv4 access	Dual Stack access (print server will support IPv6)	IPv6 access	Printer supports IPv6
P2P (public)	IPv4 access (via SIP server + NAT)	IPv4 access (via SIP server + NAT)	IPv6 access (via SIP server and P2P)	IPv6 access (via SIP server and P2P)	Framework used for P2P
P2P (specific)		IPv6	IPv6	IPv6	
Streaming	IPv4 access	IPv4 access	IPv6 access (including multicasting)	IPv6 access (includes multicasting)	
Update tools	IPv4 access (PULL type)	IPv4 access (PULL type)	IPv4 access (PULL type)	IPv6 access (PULL+PUSH type)	Security check tool, control terminal search

Summary of security migration

Item	C: Current	N: Next	N’: Next’	F: Future	Issues
Encryption	IPsec is used by the gateway	IPsec is used by the gateway	IPsec or P2P IPsec is used by the gateway depending on the terminal	IPsec or P2P IPsec is used by the gateway depending on the terminal	Standardization of methods
Virus measures	IPv4 IDS	IPv4 IDS (IPv6 mail is prohibited)	IPv4 IDS (IPv6 mail is prohibited)	IPv6 IDS	Delay in IPv6 support by virus checkers
DoS attack measures	IPv4 SPI	IPv4 SPI	Dual Stack SPI	IPv6 IDS	Name resolution and resource block escape function collaboration
GW Firewall	IPv4 SPI	IPv4 SPI + IPv6 Filter	Dual Stack SPI	IPv6 bi-directional SPI	Implementation + Incoming control
Terminal unauthorized access protection	IPv4 Personal Firewall (PFW)	IPv4 PFW Note: IPv6 with GW	IPv4 PFW Note: IPv6 with GW	Dual Stack PFW	Implementation
Terminal access	ID/PW	ID/PW	ID/PW PKI (?)	ID/PW PKI (?)	Complicated settings

4.5 IPv6 Deployment at Dependent SOHO

4.5.1 Overview of Dependent SOHO Environment

Assumptions about dependent SOHO environment

Dependent SOHO environments include sales offices and local company offices. This environment also includes insurance and travel agencies, though those businesses are basically direct offices. Dependent SOHO environment type offices typically employ up to 10 staff and system administration services are provided by a service center, not at the offices themselves. IT skills at these offices are not high.

Offices are found in scattered locations nationwide and staff primarily work in local areas. However, these offices engage in system-like interactive communication with the headquarters. Since there are many offices, the company cannot spend a lot of money for each. In general there are no complicated servers in each office.

Current analysis of dependent SOHO environment

The terminals used are primarily PCs and the office also has business equipment such as printers and file servers, special business terminals such as host terminals and telephone/fax machines. Applications used include email, Web browsing inside an Intranet or Internet, and local communication such as print and file sharing. With regard to host (center) collaboration, transaction and file exchange are performed. With respect to communication protocols, SNA, etc. have been used but there is a tendency to migrate to Web-base use. It is expected that telephone and fax use will migrate to IP telephony systems gradually.

A center-based star type network configuration is often used. In this configuration, IP-VPN, wide-area Ethernet and Internet VPN (gateway IPsec base) are common. Smaller offices use ISDN or DA128 for connections but it seems that ADSL will become the most popular choice in future. These may be used for backup or separated into voice/information related business-related usage.

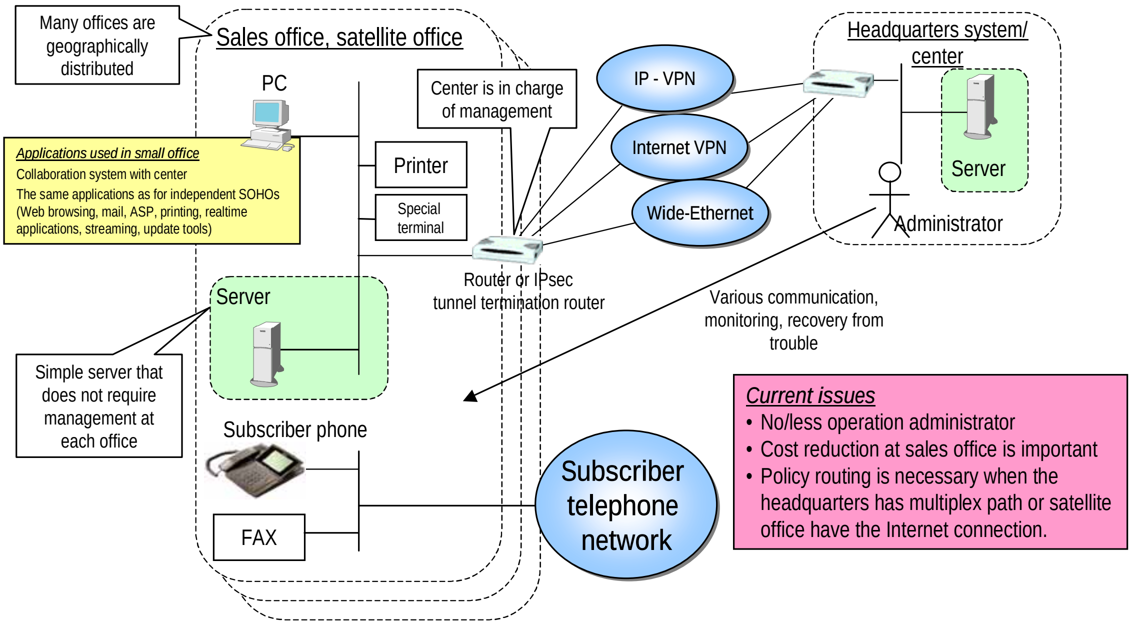
The general address structure is such that there is one WAN side address and the LAN side configures /24 private addresses. Each office uses NAT or fixed addresses on a VPN. With regard to private addressing, in some cases all offices use the same private addresses. Some require policy routing for the Internet, intranets or specific applications.

Protocols used include IPv4, NetBEUI, IPP, and file sharing protocols for local communication, and IPv4, SNA, http/SSL, POP3/SMTP, 3217, H.323/SIP, RTP and DLSW for remote communication.

Security is intensively controlled at the headquarters. Security is not usually handled by each sales office, or if it is only partial control is exercised. Gateways are used to manage line connections. Basically, there is no inward communication from the Internet. Virus check tools are already installed in terminals. In some cases, Internet communication goes through a VPN and firewall at the headquarters.

Dependent SOHO concept

Dependent SOHO concept



Many offices are geographically distributed
Sales office, satellite office
PC
Center is in charge of management
Printer
Special terminal
Router or IPsec tunnel termination router
Server
Subscriber phone
FAX
Simple server that does not require management at each office
IP - VPN
Internet VPN
Wide-Ethernet
Headquarters system/ center
Server
Administrator
Various communication, monitoring, recovery from trouble
Subscriber telephone network

Applications used in small office
Collaboration system with center
The same applications as for independent SOHOs (Web browsing, mail, ASP, printing, realtime applications, streaming, update tools)

Current issues
- No/less operation administrator
- Cost reduction at sales office is important
- Policy routing is necessary when the headquarters has multiplex path or satellite office have the Internet connection.

The dependent SOHO network configuration is similar to that of an independent SOHO environment and is characterized by connections to the headquarters system/center via such network methods as VPN.

4.5.2 Analysis of Dependent SOHO Environment Migration

Migration of a dependent SOHO environment to IPv6 is almost the same as that of an independent SOHO environment, with the difference being that the VPN must provide IPv6 support and the configuration of VPNs using IPv6 is expected. Also, it can be imagined that there would be a need for policy communication such as QoS. For details of routing with a multiple number of outward paths such as multi home, see the Tips & Tricks section.

Unlike an independent SOHO environment, dependent SOHO environments use legacy applications. For details of applications used, see the Large Enterprise Guideline.

Security is managed by a gateway at the headquarters. See the Large Enterprise Guideline for more details; note, however, that the sales office side router must be remotely managed and this issue is not covered in the Large Enterprise Guideline.

4.5.3 Migration of VPN

Analysis

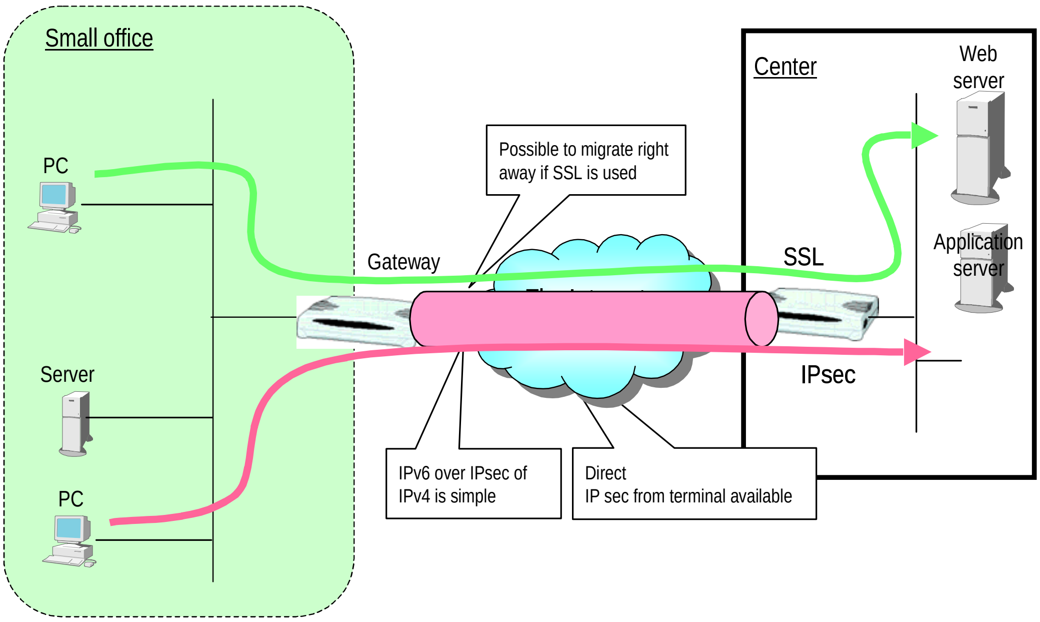
VPNs can be executed as usual without the influence of IPv6 when using SSL server on the Internet. With IPv4, it is common to use a router-based tunnel in IPsec aggressive mode.

The methods available for implementing IPv6 in a VPN includes IPv6 over IPv4 over IPsec, DTCP, IPv6 over IPsec IPv4, and IPsec IPv6 + native service. One problem with IPv6 over IPv4 over IPsec is that there are significant fragmentation effects. DTCP does not have an encryption function, thus that may result in fragmentation. IPv6 over IPsec IPv4 is a relatively low cost solution. IPsec IPv6 + native service is excellent in terms of performance and scalability.

In the near term

So, how should we deal with VPN for the time being? If it is SSL based, VPN can be used as usual by simply changing the stack to IPv6 and nothing else is required. IPv6 over IPsec IPv4 is appropriate if VPN is lightly executed in the IP layer. If scalability is emphasized, the native connection (which includes the dual stack) is appropriate.

VPN concept



Possible to migrate right away if SSL is used

IPv6 over IPsec of IPv4 is simple

Direct IP sec from terminal available

4.6 Future Usage Models

4.6.1 Overall Concept

In future, various elements will be connected to networks by IPv6.

Since there is plenty of addressing and auto settings are sophisticated, a network interface allows easy use of not only PCs, printers, IP phones and PDA, but also office equipment such as copy machines, fax machines, white boards, projectors and also peripheral PC devices, security cameras and time cards.

The spread of IPv6 may increase collaboration with external nodes. The reason for this is because streamlining of P2P communication and the security infrastructure provides better environment for external collaboration. As a result, it is expected that outsourcing of functions will increase. Collaboration examples include configuration of an order/reservation system (a Web-based system currently exists), inquiry/support desk functions, and telephone or videophone technology. Also, IPv6 will promote collaboration with users outside the company. Accompanying such development, advent of IPv6-only nodes can be expected.

Mobile access will be commonplace, for example, a user may access the SOHO from outside the office and exchange information via P2P, and information will increasingly be handled in realtime.

4.6.2 Technical Issues

Issues that must be addressed with regard to full-scale propagation of IPv6 include naming, security, QoS, securing of reliability (multi homing) and translation (who provides the function).

4.7 Summary of Requests and Issues

4.7.1 Network Issues

Network

About the number of segments in a SOHO network

What size IPv6 address is provided to a user organization is left up to the ISP. Two types of IPv6 addresses are currently distributed by ISPs, the /64 prefix (for one segment) and the /48 prefix (for multiple segments).

One advantage of a single segment /64 prefix is that configuration is easy and auto assignment functions make it easy for users as well (of course, one segment /48 prefix assignment is possible).

The advantage of operation using a /48 prefix (/64 multi segments) is that policies can be applied to each segment flexibly. On the other hand, complexity of policy management or operation management increases and management at a SOHO that does not have an administrator may become difficult.

About Prefix Delegation

In order to simplify settings in a SOHO environment in which there is no administrator, the auto setting function (called Prefix Delegation) for the network prefix from the ISP is used. Currently, there are two Prefix Delegation methods.

- **Multi-link Subnet Router (MSR) model**
  The model handles the link between the CPE (Customer Premise Equipment: ADSL modem, etc.) and the PE (Provider Edge Device) and the LAN side link of the CPE as the same link. A single /64 prefix is assigned to the LAN side terminal. This exists in theory but for the time being is not supposed to be realized in actual service. The reason for this is because it is believed a large amount of ICMP router requests (Router Solicitation) will be sent to ISPs.

- **Layer 3 router model**
  A layer 3 router that is a CPE terminates the network prefixes assigned from the ISP and distributes these assigned prefixes within the LAN side. This model can target assignment of /48 or /64 prefixes. With regard to technology based on this model, DHCPv6-PD is a major topic and RFC standardization is just around the corner (RFC recognition was completed in December 2003).

About DNS Discovery

With IPv4, the minimum amount of necessary network information (IP address, default router and DNS server address) can be obtained automatically by DHCP and actually this method is generally used.

What about network information auto setting with IPv6? IPv6 provides a way to obtain network prefixes or default router addresses by RA (Router Advertisement) from a router. However, currently DNS server addresses is not distributed by RA. For that reason, the IETF is currently discussing methods of distributing DNS server address. Candidate methods include use of Well-Known fixed address, extension of RA and extension of DHCPv6 (Stateless DHCPv6).

Notes related to applications

When the IPv6 single stack terminal/environment spreads, a translator or reverse proxy becomes necessary to access IPv4 only on the Web. These may be installed by an ISP or implementation in a home gateway may be used.

About IPv6 migration of mail software, at this moment most existing security check software does not support IPv6.

With regard to IPv6 support by ASP, it is possible that ASP that use proprietary protocols may need to modify applications.

For P2P applications, where the translation is performed is an issue when communicating between IPv4 and IPv6.

Notes related to security

With regard to security, it can be pointed out that policy setting becomes difficult as the communication style diversifies. It is expected that there will be a means to correctly set communication destination address, etc. even though no expert is available.

Essential infrastructure products such as virus checkers and personal firewalls need to support IPv6. The popularity of security at the terminal level relates to the ease with which devices can be configured.

4.7.2 Notes

MTU Discovery

With IPv4, fragmentation is possible along the path of packet delivery and ICMP such as ICMPv6 Type 2 is not used. In some cases, ICMP packets are filtered at an ISP.

On the other hand, with IPv6, fragmentation is not performed along the path of packet delivery. When the packet size becomes too big at a router along the way, the router returns an ICMPv6 Type 2 “Packet Too Big” message to the sender. The sender receives the message and repackages the packet in appropriate size and sends it again. For that reason, on the Internet, if an ICMPv6 message (at least Type2) is not delivered to the end node, communication performance may be ruined, thus care must be exercised. Therefore, care must be taken by ISPs, etc. so that ICMPv6 Type 2 messages are not filtered out.

Host name registration

As non-PC devices (cameras, printers, etc.) that can directly be connected to a network increase, people increasingly want to connect to networks easily. In SOHO environments with no administrator, about PCs, users do not want to manually register (128-bit) IPv6 addresses each time. For that reason, it is expected that a function that matches the terminal name and address will be provided.

Auto registration method for the standard host name can be said to still be in the study phase. However, available technologies include dynamic DNS, UPnP (Universal Plug and Play) and SIP. With regard to reverse search, Node Information Query of ICMPv6 is available. With this method, when a node information query (ICMPV6 Type 139) is sent to an address, a reply (ICMPv6 Type 14) including the node information (host name, etc.) is returned. Currently only UNIX's FreeBSD and Linux support this.

Application support

Currently, applications waiting for IPv6 support include DNS resolvers. The situation is that the content of the resolver supports IPv6 but communication itself does not yet support IPv6.

With regard to security tools, application gateway type virus check software (Web, mail, etc.) still does not support IPv6. However, this is not a problem because the file I/O check type software of the OS does not depend on IPv4/v6. Also, update tools such as Windows Update and messenger applications such as Windows messenger are expected to support IPv6.

QoS

Broadband increases the number of real time applications and we can imagine that spread of the IPv6 will improve P2P communication performance and the need for QoS will increase in future accordingly.

About QoS issues between PE and CPE, upstream QoS control is technically possible to some degree; however, due to cost issues, in fact it is not implemented. About downstream QoS control, it is basically difficult to do QoS from the end terminal side. However, the packet shaping function of the broadband router can realize this to some level. These issues will probably lead to requests for services and functions at the ISP side or from device venders.

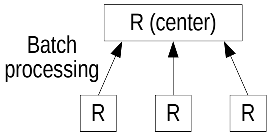
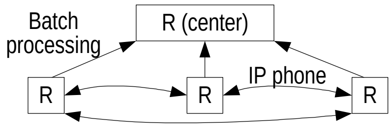
4.8 Tips & Topics

4.8.1 Change to Topology Due to Introduction of IPv6

Change to topology in dependent SOHO environments

As inter-office communication increases, mesh type configurations are also used to maintain quality.

Phenomena	Now	BCP	Future
Center (headquarters or ISP)	Connection from branch office is concentrated on client-server communication.	As broadband access is adopted in offices proceed, the processing load on center device will increase.	Only acquisition of Information at the center is provided to branch offices.
SOHO office (dependent SOHO side)	Only communicates with administrative center.	IP phone and P2P application usage will increase inter-office communication. With the star model, the administrative center is a bottleneck.	Other than cases in which connection to the administrative center is necessary, branch offices will communicate with other offices freely. VPN connection is used between offices.

Network topology change	Star (hub & spoke) type	Coexistence of star and mesh types	
Application usage style change	Branch offices only access the server at the administrative center.	With IPv6, VoIP or P2P communication is common.	Sensor network, etc. (information at branch offices is obtained via direct communication)
VPN termination change (when IPsec is used)			

(12/9) The migration from a star type configuration to a mesh type is midway through the next phase.
The bold arrow expresses the migration status.

With dependent SOHO environments, conventionally, offices only communicate with the administrative center thus the network topology is generally a star (hub and spoke) type configuration. However, as IPv6 spreads, it is believed that inter-office communication will increase. If so, we can expect that mesh type configurations will also be used to maintain communication quality.

Specifically, accompanying IPv6 migration, in addition to conventional client-server applications, is thought that use of P2P applications such as IP will increase in SOHO environments that rely on IP networks for all of their communication needs. When P2P applications are used with a conventional star type connection, there is a danger that communication in one location will cause communication quality to deteriorate. A mesh type connection that allows inter-office P2P communication is necessary to address this issue. Therefore, connection methods that allows both star and mesh type configuration is expected.

4.8.2 Multi Homing

Purpose of multi homing

The main purpose of multi homing is to appropriately use lines depending on use. For example, SNA related applications use leased lines, while Web or email uses ADSL lines. Another purpose is to secure a backup communication path. ADSL and ISDN are good candidates for such uses. Another purpose for multi homing may be load distribution or performance optimization.

Requirements by purpose

When multi homing is used to appropriate lines by type of use, one advantage is that different lines can be selected for each usage (application). It does not matter whether the need is for pull and push, if the usage is the same, it is expected that the same line will be used.

When multi homing is used for purposes of ensuring a backup communication path, we expect that another line can be used when the line becomes unavailable, and when the main line is available, the other line is not used (bi-directional) or the session is not disconnected when the line is switched.

Multi homing technology/method [outbound]

The following methods can be used to implement multi homing for outward traffic.

Setting of different gateway for each terminal

This method uses a different line for each terminal.

Sorting by terminal

Two methods can be imagined. One is a method in which the terminal sorts by itself (has a path other than the default) based on the destination address. In the other, the terminal performs policy routing (sorts by application).

Sorting by gateway (router, load distributor)

The following methods can be imagined: sorting based on destination address, policy routing (sorted by application or sender address) and performing random load distribution such as ECMP.

Inward DNS

This changes (used specially for dependent SOHO environments) the answered address according to the usage (by FQDN of the accessed address). For the purposes of backup or load distribution, multiple addresses are set.

VRRP, HSRP, ESRP etc.

Used for backup purposes. Some routers have an extension function to indicate pseudo down when line disconnection occurs.

Multi homing technology/method [inbound]

BGP

Since multi homing using BGP increases the number of paths, it is not used for large scale networks.

Support by Individual ISP

This assumes a situation in which paths go through locally between ISPs.

Technology to change addresses midway through a network

There is a technology to change addresses using NAT, proxy or tunneling.

Outward DNS

This changes answered addresses according to usage (FQDN). For the purposes of backup or load distribution, multiple addresses are set.

Multi prefix

Multiple network prefixes are set for the same link (interface). Since multiple addresses are assumption with IPv6, this method can be widely used. With pull type applications, a terminal can select the source address depending on usage.

Mobile IP

Care-of addressing is used as needed.

IPv6 multi homing

In the current IPv4 world, multi home that can be used in SOHO environments is only NAT-based. It is impossible for a SOHO to get an AS number and also punching holes is considered to be a problem. In addition, setting multiple addresses for one terminal is not common practice and is complicated. First of all, NAT is carried out even if it is not multi homing but there is a problem with this method in the use of P2P applications is difficult.

On the other hand, with IPv6, multi prefixing is thought to be an effective means. There is another method that uses RFC3718 (secondary link) but the cost is high. Especially, for dependent SOHO environments, use of multi prefixing to sort addresses by service seems to work well. For pull type applications, a source address selection function is very important. IETF’s multi6 WG is currently studying the issues and the overall idea has already been RFCed (RFC3582).

IPv6 source address selection

Source address selection is defined in RFC3484 Default Address Selection for Internet Protocol version 6 (IPv6). In this RFC, eight rules are defined for selecting sender addresses.

1. Priority is given to the same address as the address.
2. Priority is given to the nearest address to the address in terms of scope.
3. Priority is given to non-deprecated addresses.

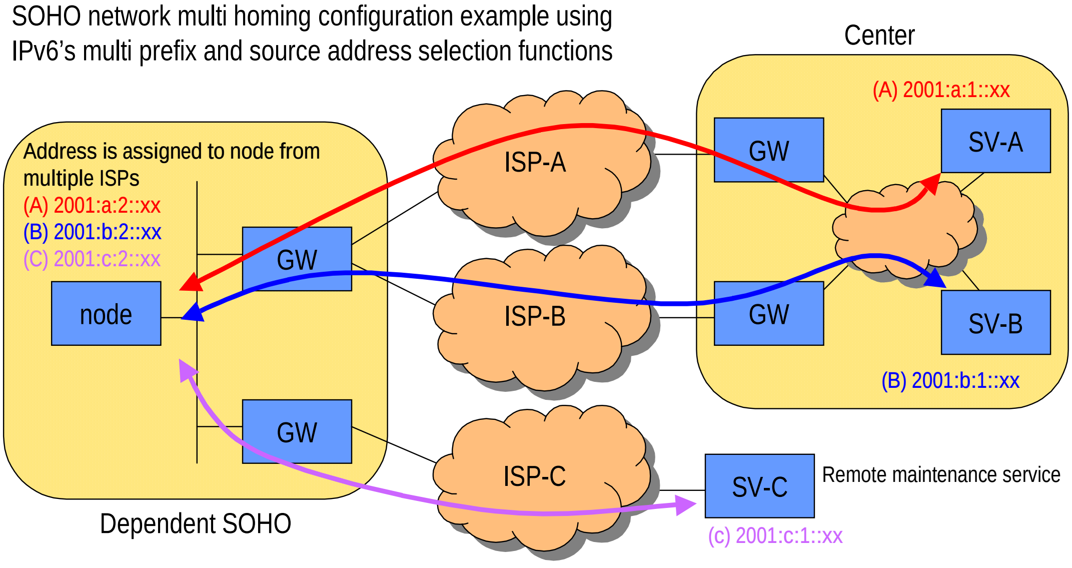
4. Priority is given to the home address rather than the care-of address. (Note: A mechanism should be provided to allow reversing by applications (SHOULD))
5. Priority is given to the address of the interface that sends that packet.
6. Priority is given to the same address as the address in terms of the label on the policy table.
7. Priority is given to the public address rather than a temporary address (Note: A mechanism should be provided to allow reversing by applications (MUST))
8. Priority is given to a address having a longer matching part with the address (called the longest match)

To appropriately use with applications, rule 8 currently can be used. However, planned address design is necessary. Rule 6 has an issue in that such an implementation requires configuration of all terminals.

Example of multi prefix / multi homing configuration

Example of multi prefix / multi homing configuration

SOHO network multi homing configuration example using IPv6's multi prefix and source address selection functions



- For a base node to access the center server, the sender address is determined by the source address selection function.
- Response from the center server to the base node is sent to the sender address of the node as is.
- The communication path from the base node and each server can be controlled in both directions.

The illustration shows the use of different sender addresses according to the accessed server address. This allows control of the communication path in both directions according to use.

Issues in multi prefix / multi homing

One issue of multi homing using multi prefix is the default router selection. When the default router is different for each line, it is unknown where data is sent. About this, RFC2461 (Neighbor Discovery) does not specifically provide a standard. When a router transfers inappropriate a packet to a line as is, it is possible that purpose is not fulfilled and also it may be caught by the ISP's ingress filter may catch it.

There are some potential solutions to this problem. One method is to modify the terminal implementation so that the corresponding sender address is looked up and the packet is sent to the RA sender router. The other method is to use draft-ietf-ipv6-router-selection-02.txt (an extension that runs a path with RA). However, until these methods become available, the only method available is to have the router side exercise redirect.

Another issue is the behavior when the line is switched. If the address is not switched immediately, communication may be interrupted because the ingress filter catches the other line's address. When a router detects line disconnection, it is better if it is reflected on RA, however, in E2E communication, the session is cut off. This is same as for NAT-based IPv4. When the line is switched, the address changes, causing session cutoff. Therefore, mobile IP, for example, requires a solution that allows the session to be maintained.

4.8.3 QoS

IP network communication quality assurance

One characteristic of the IP network is that resources are shared by allowing packet discard during competition. This allows the configuration of inexpensive IP networks.

Depending on the physical network configuration (ATM, Ethernet, etc.) that implements the IP network, different quality assurance technology is used. Also, quality thresholds differ depending on what VoIP or VPN are used for.

There are two types of quality assurance, QoS and CoS. QoS absolutely secures bandwidth, etc. CoS assigns priority order to packet transfer and packet discard and ensures relative communication quality. Technologies that ensure QoS includes QoS signaling (RSVP, etc.), packet marking, packet classifying, packet metering, packet policing, scheduling (WFQ, etc.), and cue length management (WRED, CAR, etc.).

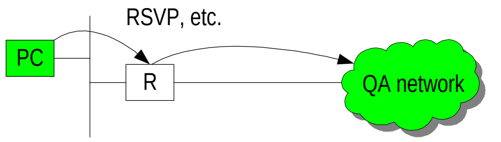
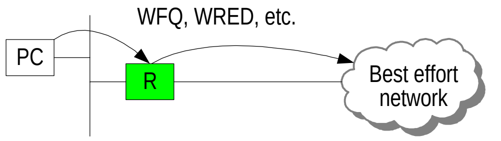
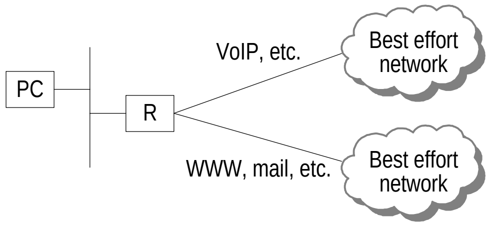
SOHO communication quality assurance

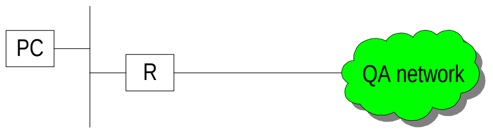
For SOHO environments, since it is relatively easy to set up Gigabit Ethernet networks, there is no need to ensure LAN quality. However, this is not the case when high value-added servers are placed in SOHO environments such as a design office.

Additionally, the smaller bandwidth used by a WAN than that used by a LAN can affect quality. Thus studying mostly WAN technology is important for SOHO quality assurance.

SOHO communication quality assurance pattern

Four patterns of communication quality assurance are used in SOHO environments. These configurations are used by themselves or in combination to realize quality assurance.

Item	Description	Basic configuration
Terminal	Terminal-initiative communication quality assurance system is used.	
Connected line	Quality assurance setting (prioritized transfer and packet discard) by router. Increase in the connected line band is included.	
Multiple connected lines	Multiple connected lines are used to distribute load.	 VoIP, etc. Best effort network PC R WWW, mail, etc. Best effort network

Communication quality ensured network	Carrier provides a network for which communication quality is ensured.	

Characteristics of IPv6 quality assurance

IPv6 quality assurance depends on the quality assurance function of the existing IP network component devices and the communication quality assurance function is not superior compared to IPv4. However, it seems fine granularity or no packet fragmentation through QoS measures by the header format are effective in reduce load on devices on the communication path.

With IPv6, the traffic class field (8 bits) provided to the header can be used for class classification of prioritized control, etc. Equivalent functionality to this in IPv4 is ToS (Type of Service) (8 bits). In addition, a field called the flow label (20 bits) is also provided. This field can be used by the sender to specify the processing method used by the flow unit.

Related to communication quality assurance, it is necessary to note that with IPv6, packet fragmentation is not performed by devices on the communication path. In order for a transmission terminal to send a packet of a size that is not discarded, an ICMP "Packet Too Big" message must reach the sender from the device on the path in which the smaller MTU is set. To do so, it is necessary to study issues such as ensuring that ISPs, etc. that manage the devices on the path do not block the said message and that there is no drop in security as a result of non-blocking.

IPv6 characteristics by phenomenon

Item	IPv4	IPv6
Communication quality assurance by application	In the IP layer, 8 bit (ToS) type control is possible.	In the IP layer, 8+24bit (Traffic Class and Flow Label) type control is possible.
Terminal-basis communication quality assurance (VoIP, remote maintenance, etc.)	Due to address mask using NAT, E2E QoS assurance is difficult.	E2E QoS assurance is easy using global addressing.
Resource guidance by terminal itself	Static resource guidance by setting path to resources beforehand or using signaling of RSVP, etc.	Dynamic resource guidance using source address selection by multi prefix.
Avoidance of processing delay caused by packet fragmentation	Processing delay increases because packet fragmentation and rebuilding occur on the communication path.	Processing delay on the path is reduced because packet fragmentation does not occur in locations other than at the sender.

Note: With IPv6, finer granularity of QoS assurance is realized thus highly flexible setting (E2E's QoS mapping, etc.) is possible.

As shown in the table, QoS and CoS mechanisms that allow fine setting are provided in IPv6 and fine granularity segmentation of assurance is realized, thus flexible operation is possible.

Summary of communication quality assurance discussion

IP communication quality assurance greatly depends on the configured physical network. Since the physical network is not changed in the course of migration from IPv4 to IPv6, we believe quality assurance technology itself will not change. However, when comparing IPv6 and IPv4, IPv6 has the advantage of quality assurance in terms of fine granularity, E2EQoS, resource guidance and packet fragmentation. Using IPv6, realization of quality assurance targeting E2E such as VoIP and remote maintenance is easy. For that reason, quality assurance through collaboration of all of the component elements on E2E is possible. However, in SOHO environments, one issue that must be addressed is that there is no administrator who designs, configures and manages quality assurance efforts.

Communication quality guideline

Accompanying migration to IPv6, it is essential for SOHO environments that rely on the IP network for the entire communication needs to ensure quality by separating mission critical communication from other non-critical communication. Using IPv6, in SOHO environments that do not have an administrator, though segmentation of quality assurance is improved and LAN quality assurance is relatively easy, managing WAN quality assurance is difficult. Therefore, automated communication quality assurance must be provided to SOHO environments. (Note: Depending on the usage method, either metered rate charging or constant rate charging is used.)

4.8.4 Device Monitoring / Remote Control

Demand for device monitoring and remote control

Demand for monitoring or controlling remote devices arises from the need for outsourcing of management. Good example of outsourcing of business by small entities is the remote monitoring of elevators. Medium and small scale buildings do not usually have a central monitoring room such as a security and disaster prevention center that is manned 24 hours a day, thus an elevator monitoring system may be used.

Another example of monitoring of devices in a network is a printer health check system (which checks the print counter and toner and paper usage to automatically order toner and paper when needed or provide periodic maintenance), providing a business opportunity for someone.

One aspect of SOHO environments is that it is easy to outsource management work. This also means there are many cases where work must be outsourced, which often makes it abundantly clear that the management level is improved. To implement remote monitoring and control service, communication between devices on the LAN and outside devices is necessary.

Device monitoring and remote control type

There are two types of remote monitoring/control, a pull type and a push type.

With the pull type, only devices inside the LAN can be an initiator and such use is easy to implement in the conventional security framework. Disadvantages, however, include communication delays and wasteful consumption of bandwidth.

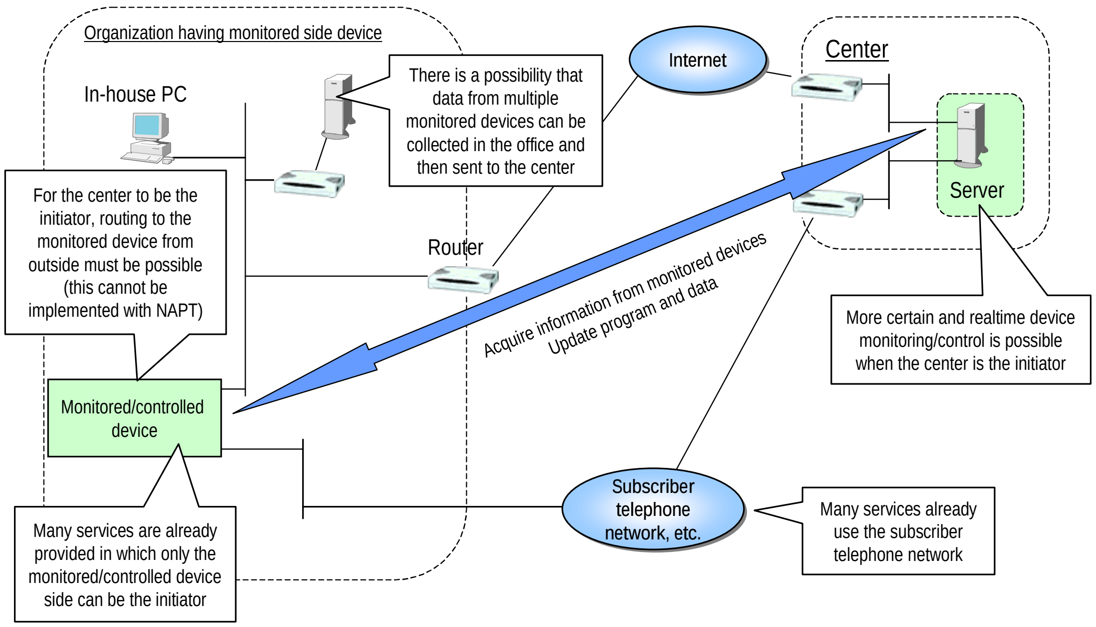
On the other hand, with the push type, not only devices inside the LAN but also devices outside the LAN can be the initiator. This type of system is very likely to be realized using IPv6, allows routing from outside and will probably create a variety of new business opportunities.

A bad example of pull type application is Windows Update. Since this is a user-initiated semi-automatic method, problems often occur, such as that users do not realize updates are necessary and cannot patch security holes. On the contrary, push type applications can directly control devices from outside. It is possible to using a pull type application to realize this on a pseudo basis, but bandwidth is wasted in such a case.

Device monitoring/remote control concept

The concept of device remote monitoring and remote control in SOHO is shown in the illustration below.

Device monitoring / remote control concept



Organization having monitored side device
In-house PC
Internet
Center
Server
Router
Acquire information from monitored devices
Update program and data
Subscriber telephone network, etc.

There is a possibility that data from multiple monitored devices can be collected in the office and then sent to the center

For the center to be the initiator, routing to the monitored device from outside must be possible (this cannot be implemented with NAPT)

Monitored/controlled device

More certain and realtime device monitoring/control is possible when the center is the initiator

Many services are already provided in which only the monitored/controlled device side can be the initiator

Many services already use the subscriber telephone network

Disadvantages of pull type applications and advantages of push type

The disadvantages of the pull type can be explained using the example of the current Windows Update. Since the pull type depends on user action, application of security patches may be delayed or many not be applied at all. Blaster and Nimda, etc. are still out there as proof of that. If Windows Update were a push type application, communication would reach the other party without delay and things that are not updated at the center side can be managed. In such a case, update CDs could be sent free of charge to only those environments where updates cannot be performed. Especially, for real time control services such as outsourcing of server management (telnet to the server from outside), it cannot be avoided that outside devices are the initiator.

Networks used for monitoring

The following measures can be used for monitoring

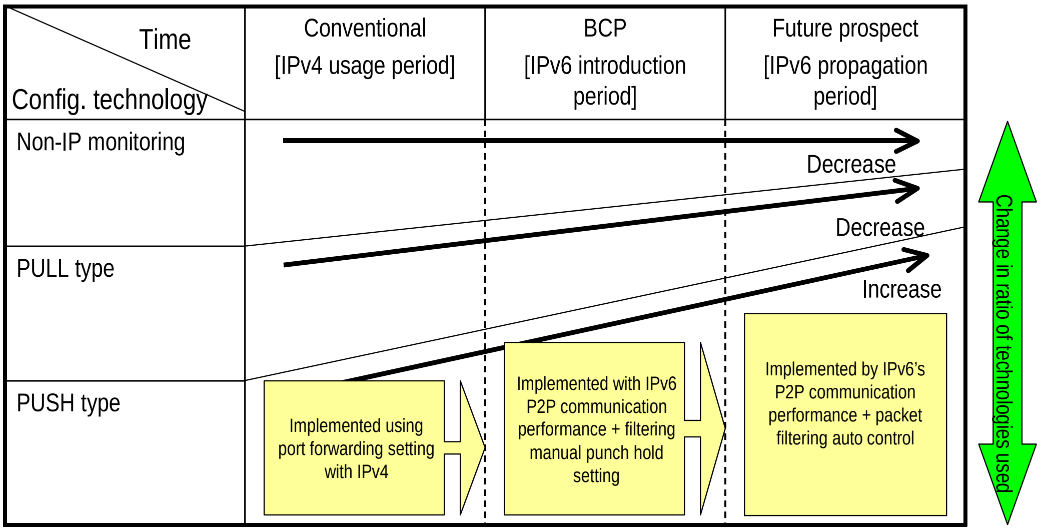
1. Non-IP network (telephone, etc.)
   Price is high and transparent communication by IP is difficult to do.
2. Leased line / wide-area Ethernet network / IP-VPN network, etc.
   Poor cost effectiveness unless the scale is large and management is troublesome
3. Internet VPN network
   Price is cheap, tunneling disadvantages, requires budget for devices
4. Monitoring communication in IPsec transport mode
   Extremely cheap, requires push type communication, easy to manage if E2E communication path is secured

From a cost and usability aspect, it is expected that a shift from 1 to 4 will occur in future.

Change in technologies used to configure device monitoring path

From the current IPv4 use period to future prospective IPv6 propagation period, the change in technologies used to configure a device monitoring path may be similar to the steps described below.

Change in technologies used to configure device monitoring path



Time
Config. technology
Conventional [IPv4 usage period]
BCP [IPv6 introduction period]
Future prospect [IPv6 propagation period]
Non-IP monitoring
PULL type
PUSH type
Decrease
Decrease
Increase
Implemented using port forwarding setting with IPv4
Implemented with IPv6 P2P communication performance + filtering manual punch hold setting
Implemented by IPv6's P2P communication performance + packet filtering auto control
Change in ratio of technologies used

Conventional technology using IPv4

For pull type services in an IPv4 environment, the initiator is always only inside the LAN thus implementation is easy. On the other hand, to implement push type applications in IPv4, we need non-IP lines, leased lines or an IP-VPN network. That means that, in order to only monitor terminals, we must connect a different network. This is expensive and cannot be used in an environment unless the monitoring system is large scale. (It is difficult to use this method for SOHO environments.)

Push using port mapping is another option. In this method, port forwarding is performed to the concerned internal node, scalability needs to be considered and higher level network management skills are required.

Change in conventional technology by IPv6 (BCP)

When migration to IPv6 starts, what kind of changes are brought to remote monitoring and control?

With regard to pull type applications, the technologies used are the same as those used with IPv4. About push type applications, the technologies used are the same as those used with IPv4 only with regard to push via a non-IP line, leased line or IP-VPN network. However, making use of IPv6's P2P communication performance, the same functionality can be implemented not only using non-IP lines but also over the Internet without requiring special settings.

Note that security considerations such as packet filter settings are necessary and settings that allow limited reachability from outside are expected. This setting has low scalability and requires a higher level of technical skill. IPsec transport mode communication by E2E can be used as well.

Future expected technologies

In future, it is expected that we will see automation of implementation of limited reachability by push that used to be done manually in BCP. Specifically, automatically implementing the following processing is expected: authentication of the other party, punching holes in filters and closing holes after use is completed.

We want to exercise control according to the other party of communication (depending on the authentication result) and control according to the communication status. To accomplish that, it is thought that a protocol similar to SIP will be used. About such a mechanism, the procedure needs to be standardized. Otherwise, the proprietary standard of makers may proliferate, increasing the cost to users. On the contrary, if this mechanism is realized, the need for other methods will decrease.

Security issues

With regard to security, allowing routing from outside to inside generates some issues. However, we can say this can be solved by doing the natural thing, that is, setting up filters. In order to give limited access permission from outside to inside, in addition to a conventional filter that is statically set, it is expected to use dynamic filters based on specified conditions, for example, when a filter receives a request from a terminal communication is permitted as needed at that moment.

In addition, the need for communication confidentiality is increasing. This causes us to put not only the conventional layer 4 or higher security into play but also layer 3 IPsec.

Concerning information leaks from devices installed inside a SOHO environment, we can take measures such as making it essential that devices perform automatic self updating and also providing continuous support to prevent leaks resulting from security holes in a device. Agreements between enterprises and government regulations are necessary to prevent devices being implemented for malicious purposes.

5. IPv6 Deployment Guideline
(Large enterprise / Local government segment)

5.1 Introduction

This document describes general details, policies and methods that network administrators and systems integrators building and maintaining networks for large enterprises and local governments need to take into account in the coming deployment of IPv6.

The information in this document is intended not as a solution but to offer examples that readers can refer to for advice on specific management policies and constraints on the deployment of IPv6.

5.1.1 SWG Members

Chair

Tsukioka (Hitachi, Ltd.)
Sakauchi (NEC Corporation)

Members (in alphabetical order)
Hashimoto (Mitsubishi Research Institute, Inc.)
Hiroumi (Intech NetCore, Inc.)
Nakahara (NEC Corporation)
Nakai (NTT Communications Corporation)
Nishida (Ricoh Company, Ltd.)
Shirata (Hitachi, Ltd.)
Suzuki (Hitachi, Ltd.)
Tachibana (aniani.com)
Tatsuki (NEC Corporation)
Tokushige (NTT Communications Corporation)
Yamamoto (NTT East)
Yamazaki (NTT Communications Corporation)
Yoshioka (Toyota InfoTechnology Center Co., Ltd.)

5.1.2 Inquiries

For questions related to Part 1, please send email to the following address:

IPv6 Promotion Council of Japan DP-WG

wg-dp-comment@v6pc.jp

5.2 Segment Features

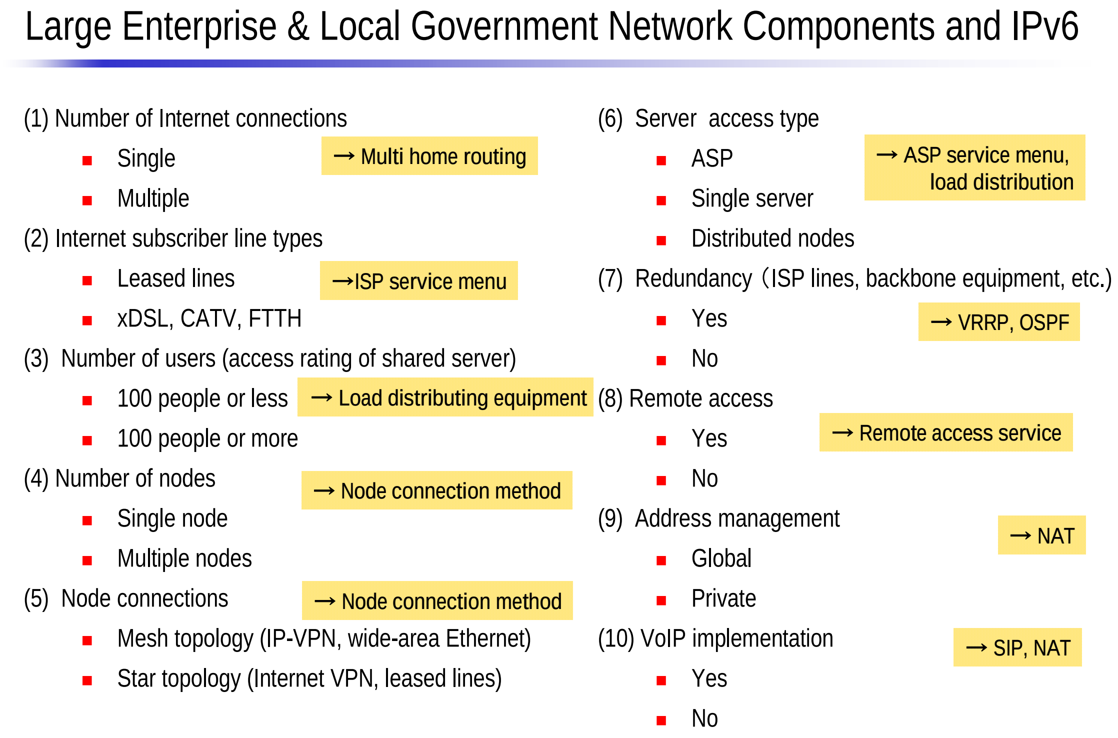
5.2.1 Features of Large Enterprises and Local Government Networks

The following describes the features of large enterprise and local government networks.

In a comparatively large network involving ten, twenty or more users a special department manages the entire network. The organization contains an intranet with mail, Web and other application services. This is the type of network that especially needs cost effective solutions.

The network department strictly maintains security policies. Redundancy configuration and periodic upgrades are performed since network equipment failures can have drastic social and organizational repercussions.

5.2.2 Large Enterprise & Local Government Network Components and IPv6



Large Enterprise & Local Government Network Components and IPv6

(1) Number of Internet connections → Multi home routing
- Single
- Multiple

(2) Internet subscriber line types →ISP service menu
- Leased lines
- xDSL, CATV, FTTH

(3) Number of users (access rating of shared server) → Load distributing equipment
- 100 people or less
- 100 people or more

(4) Number of nodes → Node connection method
- Single node
- Multiple nodes

(5) Node connections → Node connection method
- Mesh topology (IP-VPN, wide-area Ethernet)
- Star topology (Internet VPN, leased lines)

(6) Server access type → ASP service menu, load distribution
- ASP
- Single server
- Distributed nodes

(7) Redundancy（ISP lines, backbone equipment, etc.) → VRRP, OSPF
- Yes
- No

(8) Remote access → Remote access service
- Yes
- No

(9) Address management → NAT
- Global
- Private

(10) VoIP implementation → SIP, NAT
- Yes
- No

The characteristics of large enterprise and local government networks can be categorized as shown above. These characteristics affect the method of migration to IPv6 available to an organization.

5.3 BCP (what can be done now)

5.3.1 Basic Policy

The first goal is to establish the same type of environment under IPv6 that already exists under IPv4. For the time being it will be necessary to continue IPv4 and gradually phase in IPv6. Thus there is no need to convert existing applications to IPv6 but to continue to run them in the existing IPv4 network and convert them to IPv6 when upgrades are made. New applications should, for the sake of long-term future use, preferably be IPv6 compatible and be installed after adequate testing.

An IPv4/IPv6 dual stack network should be built and any partial IPv6 network should be implemented as IPv6 over IPv4 tunneling that is connected to both networks. The scope of IPv6 should then be gradually enlarged as dictated by periodic upgrades and network traffic needs.

5.3.2 BCP Security

Strict network security is an absolute must in any large enterprise and local government network. Two models to achieve such security for the time being are described below.

Relaxed model

Settings to accommodate IPv6 would be added to current IPv4 base firewall settings to and a second setting to allow separate but limited IPv6 access would be made. In the initial stage, one segment is converted to IPv6 (connected through tunneling or other means). P2P access for IPv6 applications should be introduced via the minimum required number of ports in the firewall after special examination.

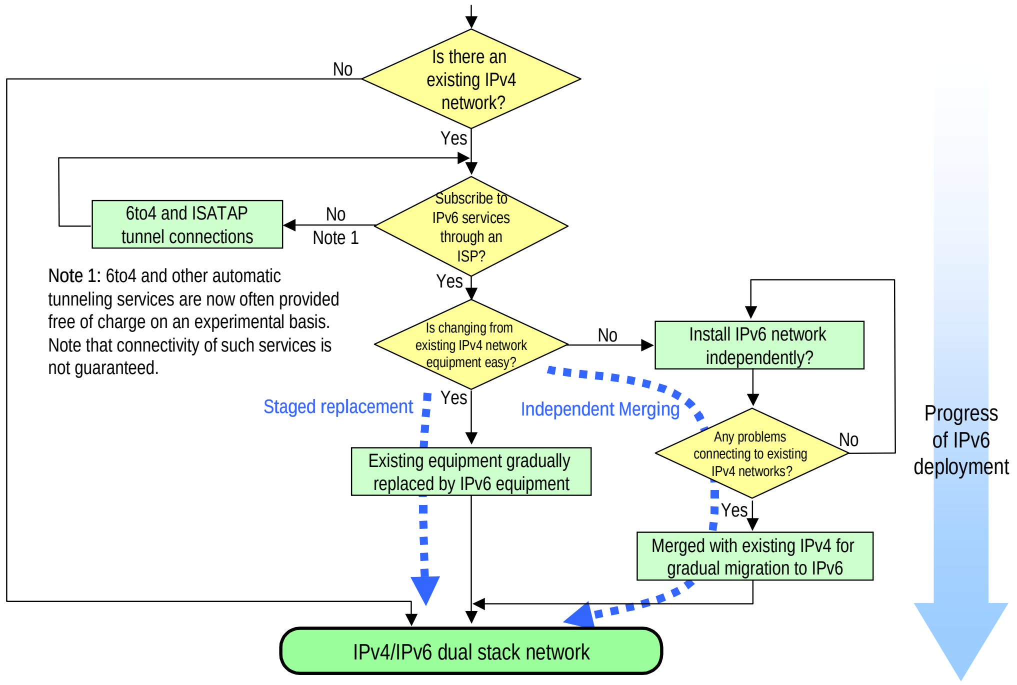
Strict model

The security policy for this model does not allow the connection of the existing network with the new IPv6 network. In the initial stage, a separate IPv6 network will be built. Until security policies for large enterprise and local government IPv6 networks reach an acceptable level, confidential business information, personal information and the like should not be handled over the IPv6 network or terminals connected to it.

Formulating an IPv6 security policy is the current top-priority issue for both large enterprises and local governments.

5.3.3 Flow of IPv6 Network Building

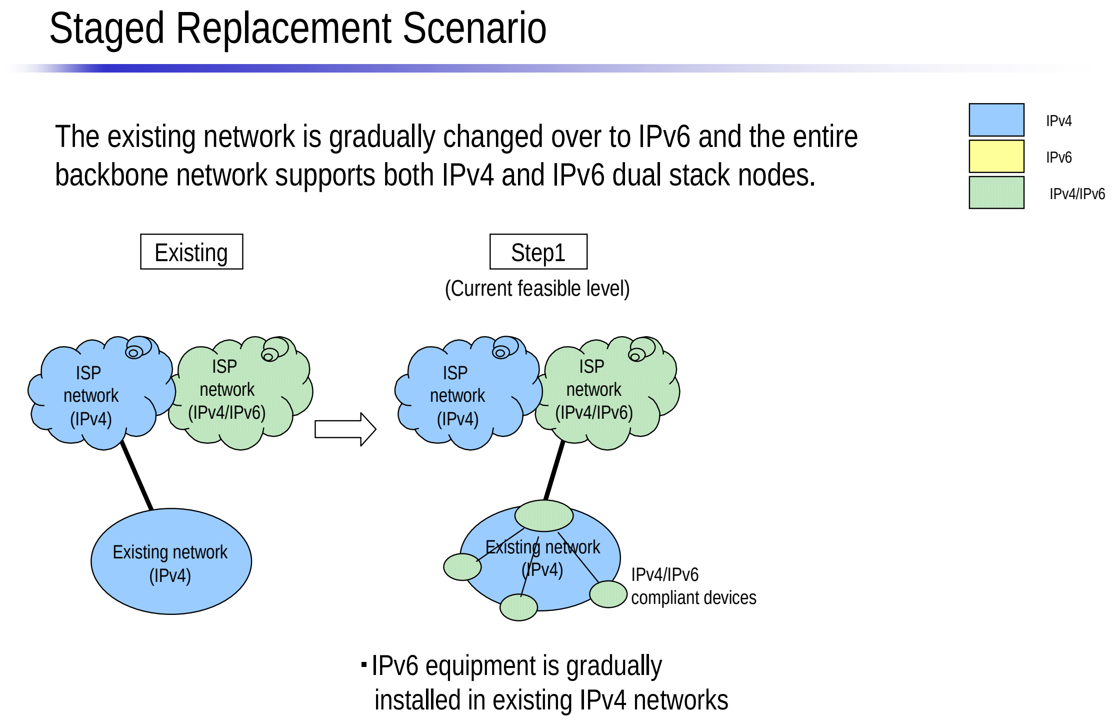
Flow of IPv6 Network Building


Is there an existing IPv4 network?
No
Yes
Subscribe to IPv6 services through an ISP?
6to4 and ISATAP tunnel connections
No
Note 1
Yes
Is changing from existing IPv4 network equipment easy?
No
Install IPv6 network independently?
Staged replacement
Yes
Independent Merging
Any problems connecting to existing IPv4 networks?
No
Existing equipment gradually replaced by IPv6 equipment
Yes
Merged with existing IPv4 for gradual migration to IPv6
IPv4/IPv6 dual stack network
Progress of IPv6 deployment

Note 1: 6to4 and other automatic tunneling services are now often provided free of charge on an experimental basis. Note that connectivity of such services is not guaranteed.

The figure above shows a schematic view of the migration to IPv6 for large enterprises. The migration to IPv6 can take two forms, either staged replacement or an independent merging process. Prior to migration, the IPv6 network can be tested before subscribing to IPv6 services.

Staged Replacement Scenario



Staged Replacement Scenario

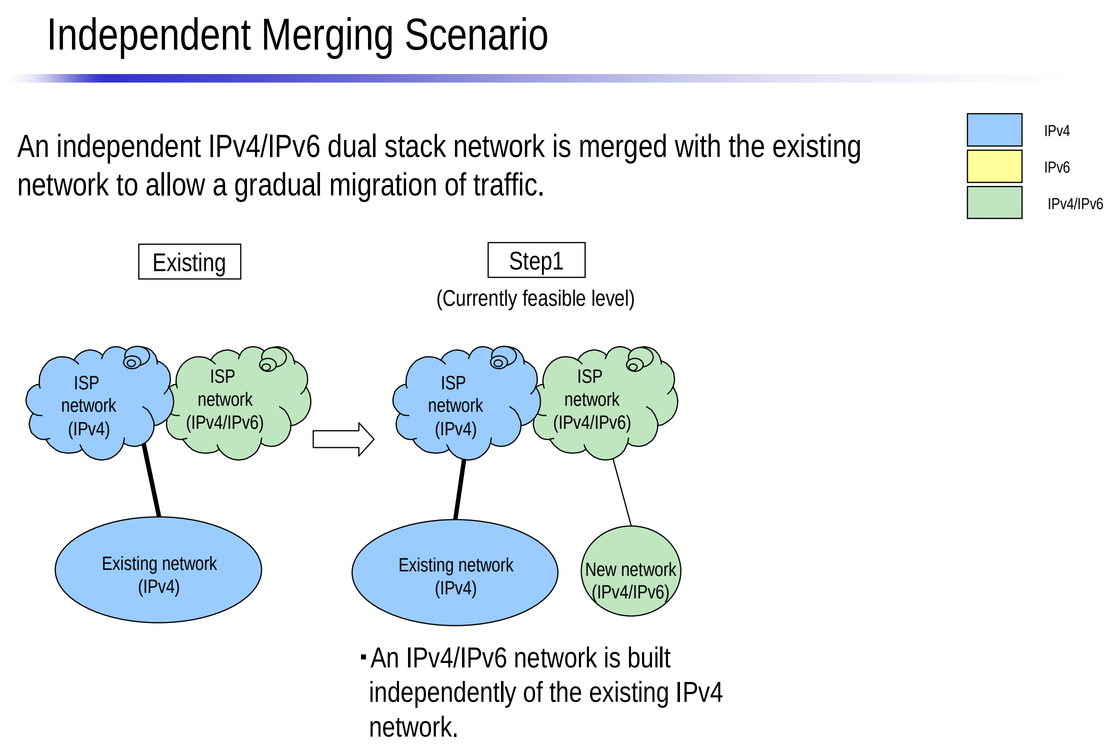
The existing network is gradually changed over to IPv6 and the entire backbone network supports both IPv4 and IPv6 dual stack nodes.

🟦 IPv4
🟨 IPv6
🟩 IPv4/IPv6

・IPv6 equipment is gradually installed in existing IPv4 networks

Here, the existing IPv4 network is gradually changed over to an IPv4 and IPv6 dual stack environment. The dual stack segment is gradually expanded to finally include the major part of the network.

Independent Merging Scenario



Independent Merging Scenario

An independent IPv4/IPv6 dual stack network is merged with the existing network to allow a gradual migration of traffic.

🟦 IPv4
🟨 IPv6
🟩 IPv4/IPv6

- An IPv4/IPv6 network is built independently of the existing IPv4 network.

This shows how a dual stack network is built independently of the existing IPv4 network. The new network is merged with the existing network and traffic is gradually moved to the new network.

5.3.4 Reasons for Deploying IPv6 Now

The following are some of the reasons why large enterprises are moving over to IPv6 now.

1. Deploying an IPv6 network environment ahead of competitors
   IPv6 is deployed as part of long-term equipment planning with the objective to enable use of future network applications ahead of the competition.
2. Deploying IPv6 by installing new IPv6 compatible applications (VoIP, etc.)
   Business trips, meetings and other business functions can be made more efficient. Work at home will also be possible.
   Security can be performed on an individual basis rather than be an organization-wide concern.
3. Setting up an environment for IPv6 development
   The objective is to develop IPv6 products.
4. Improving the corporate image, presence, marketing expertise and customer appeal
   The introduction of advanced technology is expected to improve the corporate image.

5.3.5 Deploying an IPv6 Network Environment Ahead of Competitors

IPv6 services and equipment

The basic technology required for IPv6 is already available.

ISP lines

Major ISPs have already started offering three types of services: tunnel, dual stack and native. Tunnel is the best choice to experiment with IPv6 since it limits the impact on the existing IPv4 network to a minimum. However, overhead caused by encapsulation is inevitable.

Dual stack is the choice for full-scale IPv6 implementation. At this time, the step to IPv6-only native lines is fraught with limitations since DNS and SNMP are not yet fully IPv6 compatible. Native lines are the choice for small-scale ISPs.

Routers

Most medium to large routers are IPv6 compatible (hardware processing is also making progress). Connectivity between vendor products is also high and connectivity between RIPng, OSPFv3, PIM-SM and other protocols is being tested. The progress of small routers towards IPv6 compatibility, however, is slow. Since independent IPv4 and IPv6 configurations are possible, IPv6 compatibility is a mandatory condition.

Firewalls

The basic packet filtering function in commercial firewalls is finally becoming IPv6 compatible. Functions, performance and reliability should now be tested.

The security policy that will be required for P2P applications between client terminals, IPsec communications, tunneling and multicasting is a major future issue. Firewalls that support multicast routing protocols are still to appear on the market.

DNS servers

If BIND is used, a standard upgrade will bring IPv6 compatibility. In a dual stack network, AAAA record compatibility is essential, but there is no need for DNS query packets to be converted to IPv6. For the time being, it is not essential to set up DNS capable of handling IPv6 internally, but procedures that can reference external DNS servers compatible with IPv6.

Other servers

IPv6 compatibility of Web servers and mail servers is progressing. However, in moving to IPv6, it is essential to confirm IPv6 compatibility of virus checkers and other security measures. The MIB of network management servers are IPv6 compatible while SNMP products are mostly IPv4.

PC / PDA

Major operating systems are already IPv6 compatible even if the level of functionality varies. Large enterprises can often implement IPv6 compatibility by installing the latest version of the operating system. Still thorough security measures should be taken at terminal level (by installing personal firewalls, virus scanning software, etc.) to secure end-to-end communications.

Obtaining and managing IPv6 global addresses

Obtaining IPv6 global addresses

Firms can be assigned a /48 or even a /64 global prefix by subscribing to an ISP (multiple services including commercial and testing) that provides IPv6 services. Large enterprises and local governments that intend to build a network of a certain size should obtain /48 IPv6 addresses. Refer to the Section, “Method for Assigning Local Addresses for IPv6" in Chapter 6, “Tips & Tricks” for information on how to assign addresses when experimenting with IPv6 deployment in a closed network prior to obtaining global addresses from an ISP.

IPv6 address design and operation methods

A /48 global prefix provides sufficient address space for most large enterprises and local government networks.

In IPv4, it is essential to carefully plan the number of terminals that will be needed in future when segments are made. The last 64 bits of an IPv6 address, the interface identifier, enable connection of a virtually unlimited number of terminals. Thus when obtaining a /48 global address, 16 bits can be used to make segments and there is no need to consider the number of terminals.

However, address assignment should:

- Be simple and efficient
- Take into consideration scheduled addressing based on anticipated foreseeable future changes in network configuration and size
- Be tailored to the geographical and organizational needs of the network

Routing

Status of device compatibility

Most IPv6 routers are also compatible with RIPng and advanced models support OSPFv3. Compatibility with other maker products has been verified for ease of use.

IPv6 routing protocols

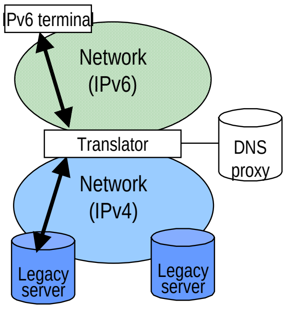
Static routing is enough in the initial stage of IPv6 deployment for large enterprise and local government networks. Install RIPng and OSPFv3 when the network grows in size. In a dual stack configuration, IPv4 routing protocols should be considered to decrease network complexity. Select devices supporting PIM-SM and other multicast routing protocols for multicast use that includes live telecasting or broadcasting services, etc.

Translators

Translators

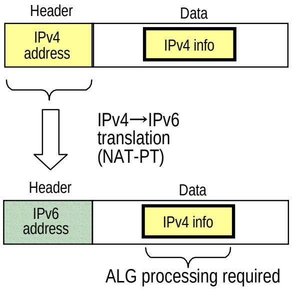
[Characteristics]

- NAT-PT and TRT translators have been commercialized.
- Protocol conversion during communications enables communications between IPv4 and IPv6 hosts.
- DNS proxies make it possible to specify destinations using FQDN (Fully Qualified Domain Name).
- Legacy system servers can be made IPv6 compatible without changing their settings. (Vast IPv4 system resources are available "as is")



[Issues]

- ALG (Application Level Gateway) is required for applications that do not conform to the seven layer model (see right).
- Packets converted from IPv4 to IPv6 require an MTU (Maximum Transmission Unit) setting.
- The destination requires an FQDN.
- Protocol conversion using reverse proxy must be differentiated from that performed by DNS proxy.



Characteristics

Most commercial translators are either NAT-PT or TRT translators. They enable communication between IPv4 and IPv6 hosts through IPv4/IPv6 protocol conversion during communications. Destinations can be specified using a DNS proxy with FQDN (Fully Qualified Domain Names). IPv6 support can thus be provided without changing the network settings of legacy systems (making vast IPv4 system resources available without modification).

Issues

Applications that infringe on the seven layer model require an ALG (Application Level Gateway). MTU (Maximum Transmission Unit) settings are also required in converting IPv4 packets to IPv6 packets. The destination requires FQDN. Occasional use of protocol conversion by reverse proxy is expected.

Tunneling

Fixed tunneling

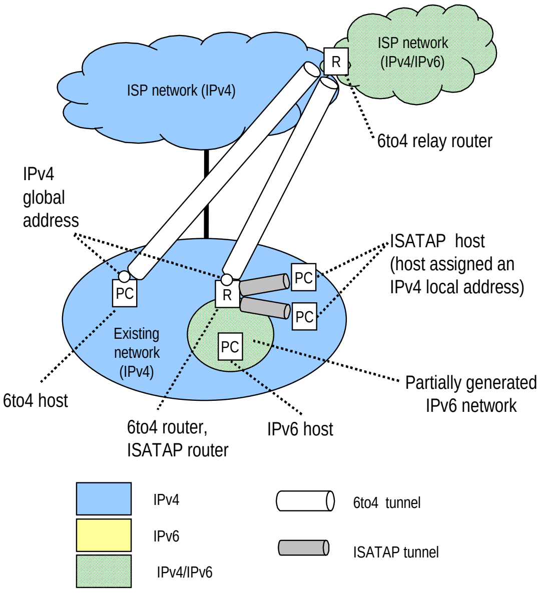
Generates a fixed IPv6 over IPv4 tunnel between specific IPv6 routers.

Automatic tunneling

- DTCP (Dynamic Tunnel Configuration Protocol)
  Enables dynamic generation of tunnels from client side. (Example: Feel6 Farm IPv6 connection experiment offered by Freebit)
- 6to4
  This mechanism automatically generates IPv6 addresses from global IPv4 addresses. Under Windows XP a 6to4 tunnel can be automatically generated by assigning a global IPv4 address to a host. It provides tunneling between 6to4 relay routers provided by major ISPs, but there is no guarantee that the outgoing path will be the same as the incoming path.
- ISATAP
  Generates a tunnel in a LAN where local IPv4 addresses are used.
- Teredo
  Enables tunnel technology in a NAT device environment.

Tunneling

[IPv6 Using Automatic Tunneling Protocols (6to4, ISATAP, etc.)]



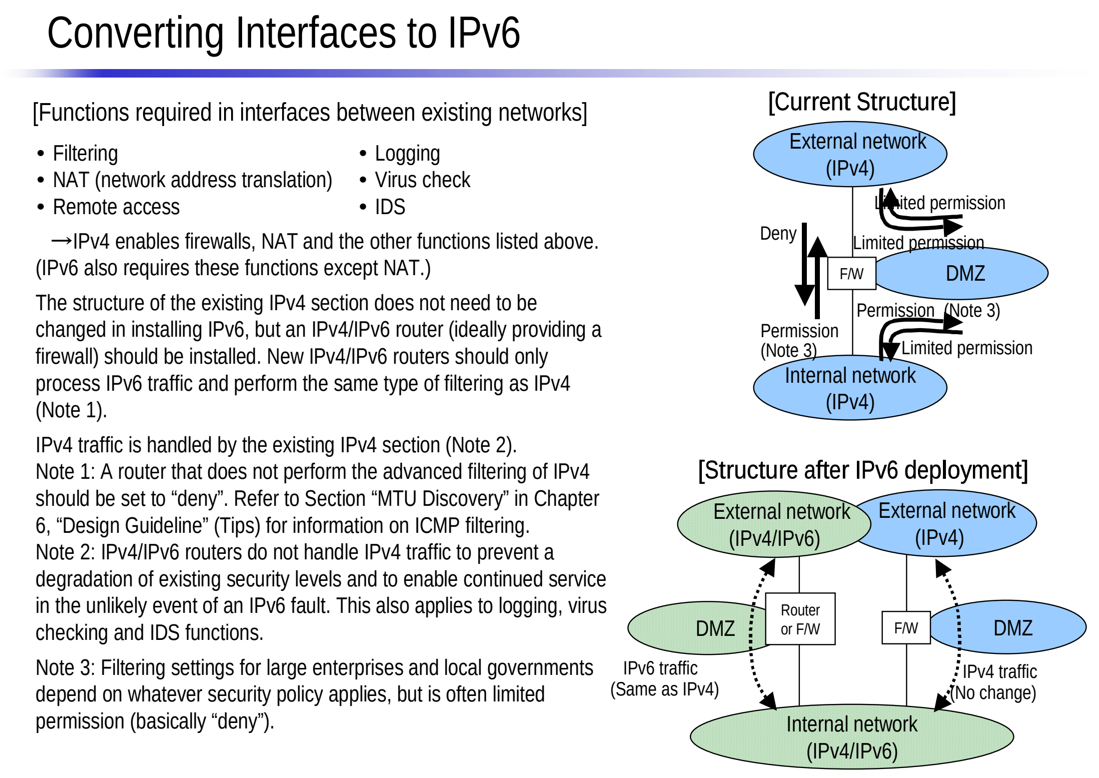
- 6to4 tunnels are generated between 6to4 relay routers available to the public and routers/hosts with IPv4 global addresses.
- ISATAP tunnels are generated between ISATAP routers (interface between IPv4 global and local addresses) and hosts without an IPv4 global address.
- A setting that lets IPv6overIPv4 packets (IP protocol no. 41 packet) through any firewall in the segment a tunnel is generated.
- IPv6 deployment is comparatively easy, however, performance, reliability and security issues still remain to be solved.
- Packets transferred in a 6to4 tunnel may not take the same route returning as going out.

Automatic tunneling protocols are used as described below.

- Generates a 6to4 tunnel between public 6to4 relay routers and routers/hosts with IPv4 global addresses
- Generates ISATAP tunnels between ISATAP routers (between IPv4 global and local addresses) and hosts without IPv4 global address

Note that while these automatic tunnel protocols provide fairly effortless deployment of IPv6, there are performance, reliability and security problems that need to be solved. Especially, if there is a firewall in the tunnel segment, settings that allow IPv6overIPv4 packets (IP protocol number 41) through the firewall must be made and this setting must consider security management issues. The outgoing path of transferred packet in a 6to4 tunnel may not be the same as the incoming path.

Converting Interfaces to IPv6



Converting Interfaces to IPv6

[Functions required in interfaces between existing networks]

- Filtering
- NAT (network address translation)
- Remote access
- Logging
- Virus check
- IDS

→IPv4 enables firewalls, NAT and the other functions listed above. (IPv6 also requires these functions except NAT.)

The structure of the existing IPv4 section does not need to be changed in installing IPv6, but an IPv4/IPv6 router (ideally providing a firewall) should be installed. New IPv4/IPv6 routers should only process IPv6 traffic and perform the same type of filtering as IPv4 (Note 1).

IPv4 traffic is handled by the existing IPv4 section (Note 2).
Note 1: A router that does not perform the advanced filtering of IPv4 should be set to “deny”. Refer to Section “MTU Discovery” in Chapter 6, “Design Guideline” (Tips) for information on ICMP filtering.
Note 2: IPv4/IPv6 routers do not handle IPv4 traffic to prevent a degradation of existing security levels and to enable continued service in the unlikely event of an IPv6 fault. This also applies to logging, virus checking and IDS functions.

Note 3: Filtering settings for large enterprises and local governments depend on whatever security policy applies, but is often limited permission (basically “deny”).

Functions required at the interfaces between existing networks include filtering, logging, NAT (address conversion), virus checking, remote access, IDS, etc. In IPv4, firewalls and NAT devices were charged with these functions. IPv6 also needs these functions, except NAT (address conversion). It is ideal to install an IPv4/IPv6 router (if possible a firewall) when deploying IPv6 rather than modifying the existing IPv4 segment. Recent IPv4/IPv6 routers only process IPv6 traffic and should be set to perform the same type of filtering as IPv4 (Note 1). IPv4 traffic is processed by the existing IPv4 segment (Note 2).

Note 1　Set to “Deny” if the advanced filtering equivalent to IPv4 cannot be provided. Refer to the Section, “MTU Discovery” in “Design Guideline” (Tips) for information on ICMP filtering.

Note 2　IPv4/IPv6 routers do not handle IPv4 traffic to prevent a degradation of existing security levels and to enable continued service in the unlikely event of an IPv6 fault. This also applies to logging, virus checking and IDS functions.

Note 3　Filtering settings for large enterprises and local governments depend on whatever security policy applies, but is often limited permission (basically "deny").

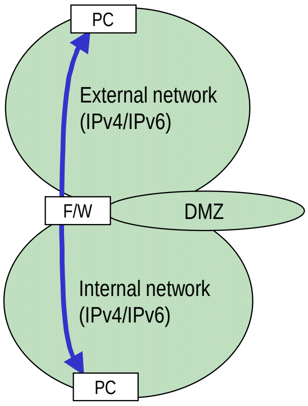
Filtering

Filtering (1) Firewalls compatible with IPv6

IPv4 and IPv6 should maintain the same security policies (and prevent degradation).

[E2E Communications]

- E2E communications through a firewall must be limited to specific terminals and access must be restricted (via filtering based on IP address and port number).
- IPsec based E2E communications through a firewall is a future issue. (Tests with IPsec communications should be limited to specific terminals and allow access of specific senders (based on IP address filtering). The receiving terminals should be protected by a personal firewall.)



Firewalls compatible with IPv6

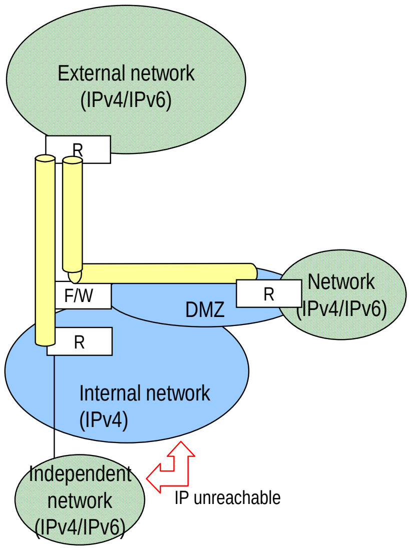
If an IPv6 firewall is used, it should maintain the same security policy for both IPv4 and IPv6 (or at least ensure that there is no degradation of security). End-to-end communications through the firewall must be limited to specific access of specific terminals (filtered based on IP address and port number). IPsec based end-to-end communications through the firewall will be provided at a later date. (If provided on an experimental basis, it should again be limited to specific access of specific terminal (filtered based on IP address). The terminals should be protected by personal firewalls.)

Firewalls not compatible with IPv6

Filtering (2) Firewalls not compatible with IPv6

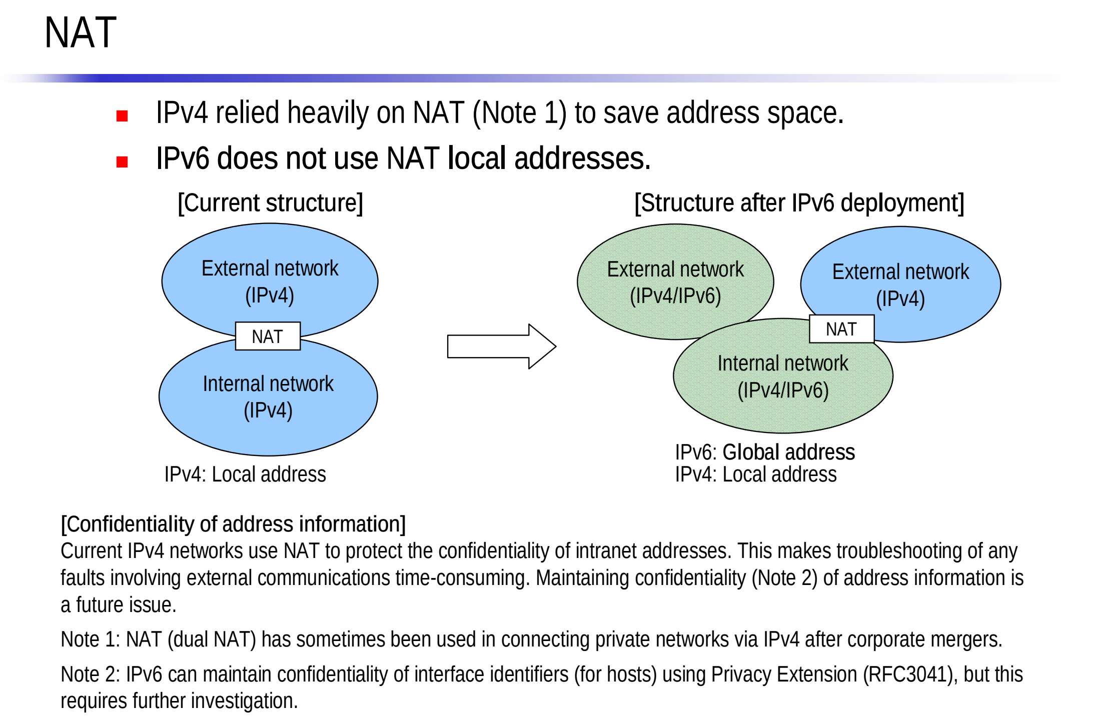
[IPv6overIPv4 tunnel]

- IPv6overIPv4 tunnel allows access to DMZ (IP protocol number 41) to generate a partial IPv6 segment in DMZ. This IPv6 segment must restrict host connections and perform special security management.
- IPv6overIPv4 tunnel communications should be allowed into a network independent (IP unreachable) of the existing internal network (passing through IP protocol number 41).



If a firewall not compatible with IPv6 is used, it should allow IPv6overIPv4 tunneling access to DMZ (enabling passage of IP protocol number 41) and generate a partial IPv6 segment in DMZ. This IPv6 segment must be restricted to specific hosts and be subject to a special security management scheme. For the time being, any experimental IPv6 over IPv4 tunnel communications accessing the internal network (via IP protocol number 41) must be limited to networks (both of which are IP unreachable) that are separate from the existing network.

NAT



NAT

- IPv4 relied heavily on NAT (Note 1) to save address space.
- IPv6 does not use NAT local addresses.

[Confidentiality of address information]
Current IPv4 networks use NAT to protect the confidentiality of intranet addresses. This makes troubleshooting of any faults involving external communications time-consuming. Maintaining confidentiality (Note 2) of address information is a future issue.

Note 1: NAT (dual NAT) has sometimes been used in connecting private networks via IPv4 after corporate mergers.

Note 2: IPv6 can maintain confidentiality of interface identifiers (for hosts) using Privacy Extension (RFC3041), but this requires further investigation.

IPv4 made heavy use of NAT to save address space (Note 1). As a rule, IPv6 does not use local addresses or NAT.

A conventional IPv4 network used NAT to maintain the confidentiality of intranet address data. The problem was that any fault occurring in communications with external hosts became far more complicated to clear up. Maintaining the confidentiality of address data in the new network (Note 2) is another issue that will have to be solved.

Although the insecurity that system administrators feel when using global addresses is an argument against using them, there were numerous examples of intranets in the USA using global addresses prior to the introduction of CIDR. Measures to remove such fears must be considered.

Note 1 NAT (dual NAT) has sometimes been used in connecting private networks via IPv4 after corporate mergers.

Note 2 IPv6 can maintain confidentiality of interface identifiers (hosts) using Privacy Extension (RFC3041), but this requires further investigation.

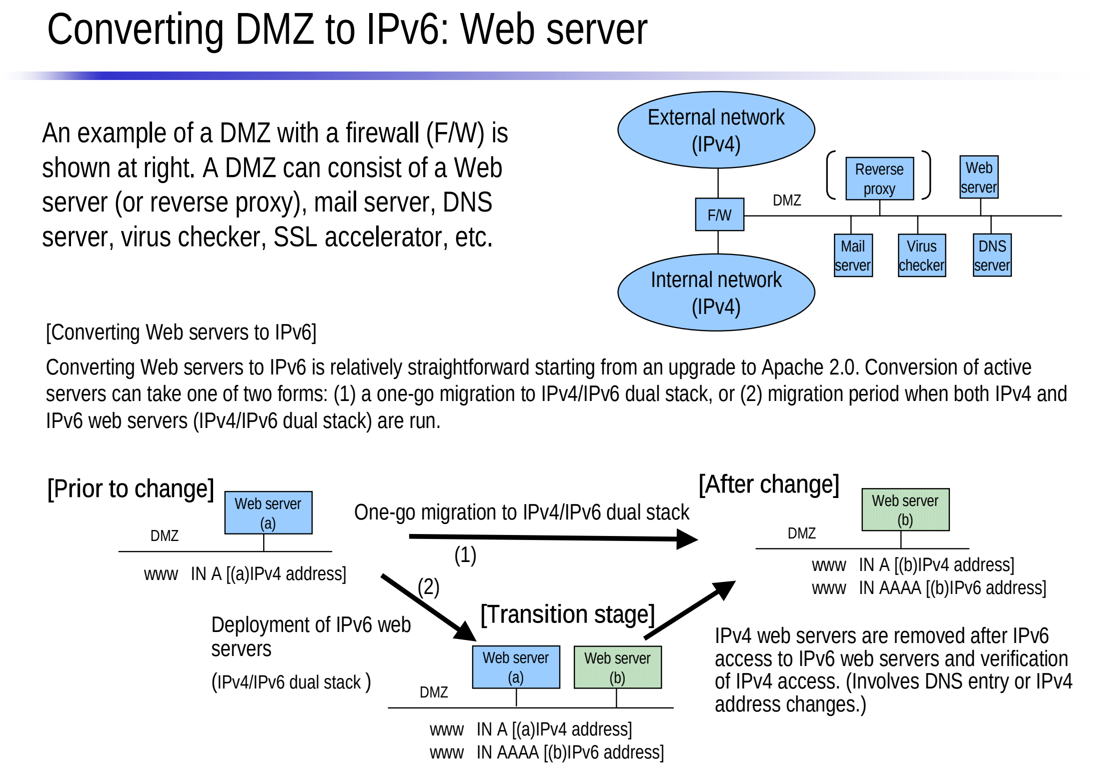
Remote Access

Remote access currently take the following forms:

1. Phoning the company owned NAS
2. Phoning the service provider NAS and making L2TP access from there
3. Using Internet VPN (tunnel mode)
4. SSL-VPN

The best way to perform IPv6 remote access is to generate an IPv6 tunnel on top of IPv4 remote access. However, the fragmentation that IPv6 over IPv4 over IPv4 (security channel) results in must be taken into account.

Converting DMZ to IPv6: Web Servers



Converting DMZ to IPv6: Web server

An example of a DMZ with a firewall (F/W) is shown at right. A DMZ can consist of a Web server (or reverse proxy), mail server, DNS server, virus checker, SSL accelerator, etc.

[Converting Web servers to IPv6]

Converting Web servers to IPv6 is relatively straightforward starting from an upgrade to Apache 2.0. Conversion of active servers can take one of two forms: (1) a one-go migration to IPv4/IPv6 dual stack, or (2) migration period when both IPv4 and IPv6 web servers (IPv4/IPv6 dual stack) are run.

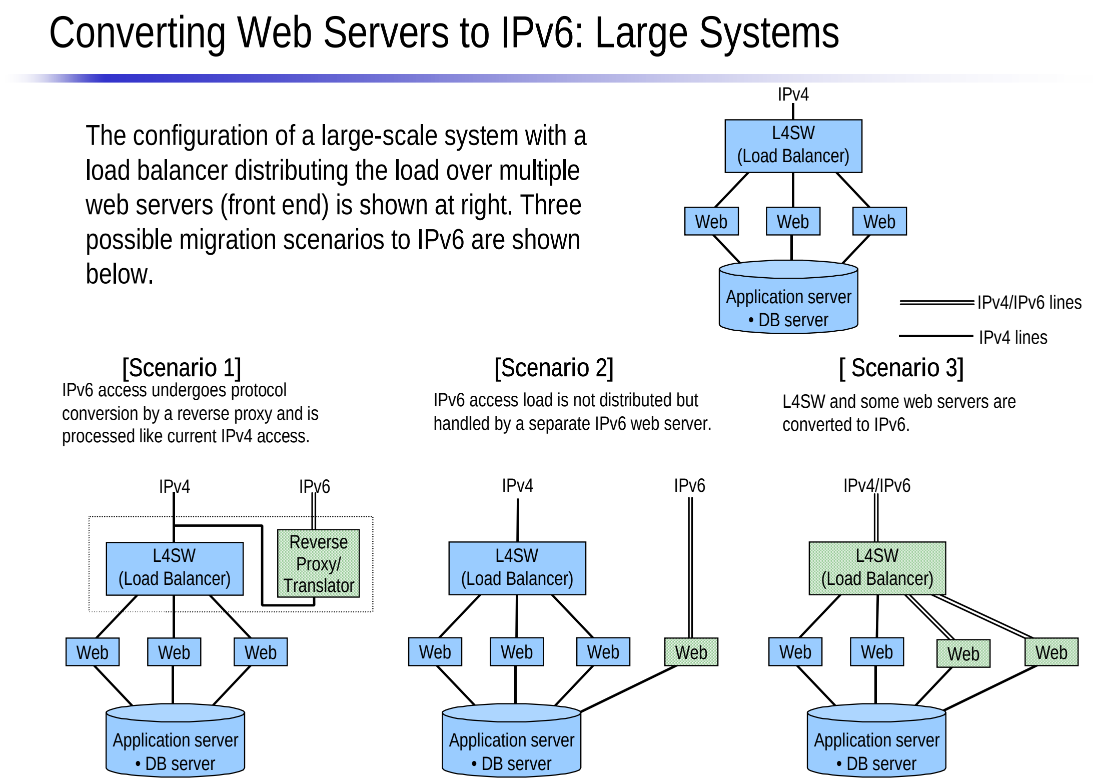
[Prior to change]
Web server (a)
DMZ
www IN A [(a)IPv4 address]
One-go migration to IPv4/IPv6 dual stack
(1)
(2)
[After change]
Web server (b)
DMZ
www IN A [(b)IPv4 address]
www IN AAAA [(b)IPv6 address]
Deployment of IPv6 web servers
(IPv4/IPv6 dual stack)
[Transition stage]
Web server (a)
Web server (b)
DMZ
www IN A [(a)IPv4 address]
www IN AAAA [(b)IPv6 address]

IPv4 web servers are removed after IPv6 access to IPv6 web servers and verification of IPv4 access. (Involves DNS entry or IPv4 address changes.)

An example of a DMZ firewall configuration is shown above. A DMZ often contains a Web server (or a reverse proxy), mail server, DNS server, virus checker, SSL accelerator, etc.

A Web server, such as Apache 2.0, can fairly easily be converted to IPv6 through an upgrade. Two scenarios are available for conversion of an active Web server to IPv6. (1) Convert to IPv4/IPv6 dual stack or (2) run an IPv4 Web server alongside an IPv6 Web server (IPv4/IPv6 dual stack) for a period of time.

Converting Web Servers to IPv6: Large Systems



Converting Web Servers to IPv6: Large Systems

The configuration of a large-scale system with a load balancer distributing the load over multiple web servers (front end) is shown at right. Three possible migration scenarios to IPv6 are shown below.

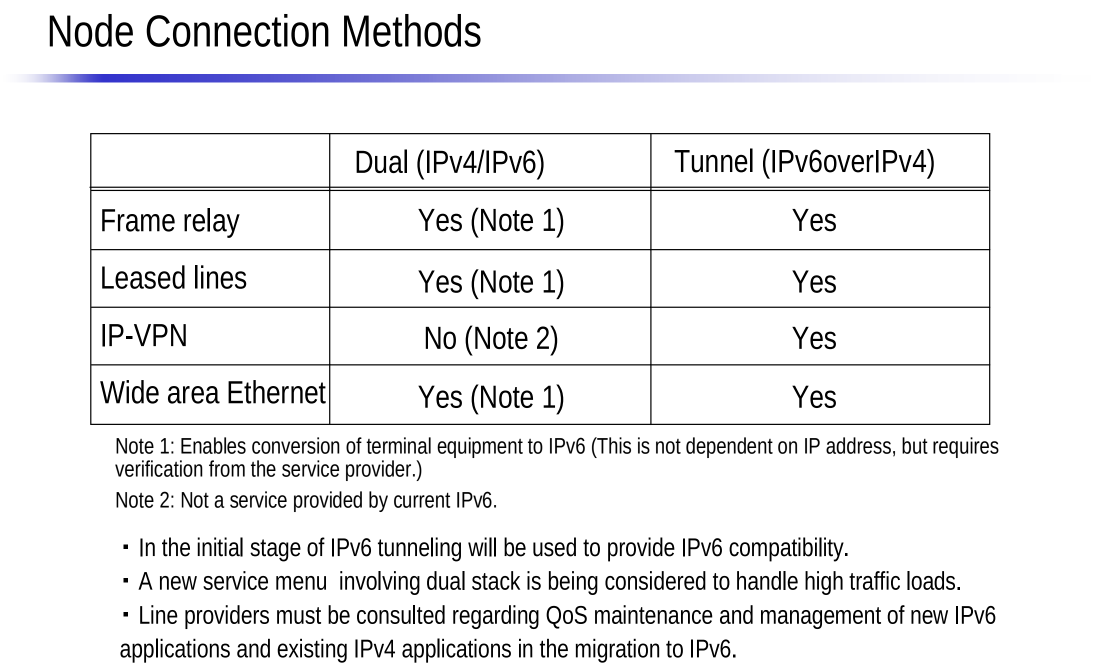
[Scenario 1]
IPv6 access undergoes protocol conversion by a reverse proxy and is processed like current IPv4 access.

[Scenario 2]
IPv6 access load is not distributed but handled by a separate IPv6 web server.

[Scenario 3]
L4SW and some web servers are converted to IPv6.

As shown above, a load balancer is used in large systems to distribute the load between multiple Web (front end) servers. Migration to IPv6 can be performed as shown by scenarios 1 to 3.

Node Connection Methods



Node Connection Methods

	Dual (IPv4/IPv6)	Tunnel (IPv6overIPv4)
Frame relay	Yes (Note 1)	Yes
Leased lines	Yes (Note 1)	Yes
IP-VPN	No (Note 2)	Yes
Wide area Ethernet	Yes (Note 1)	Yes

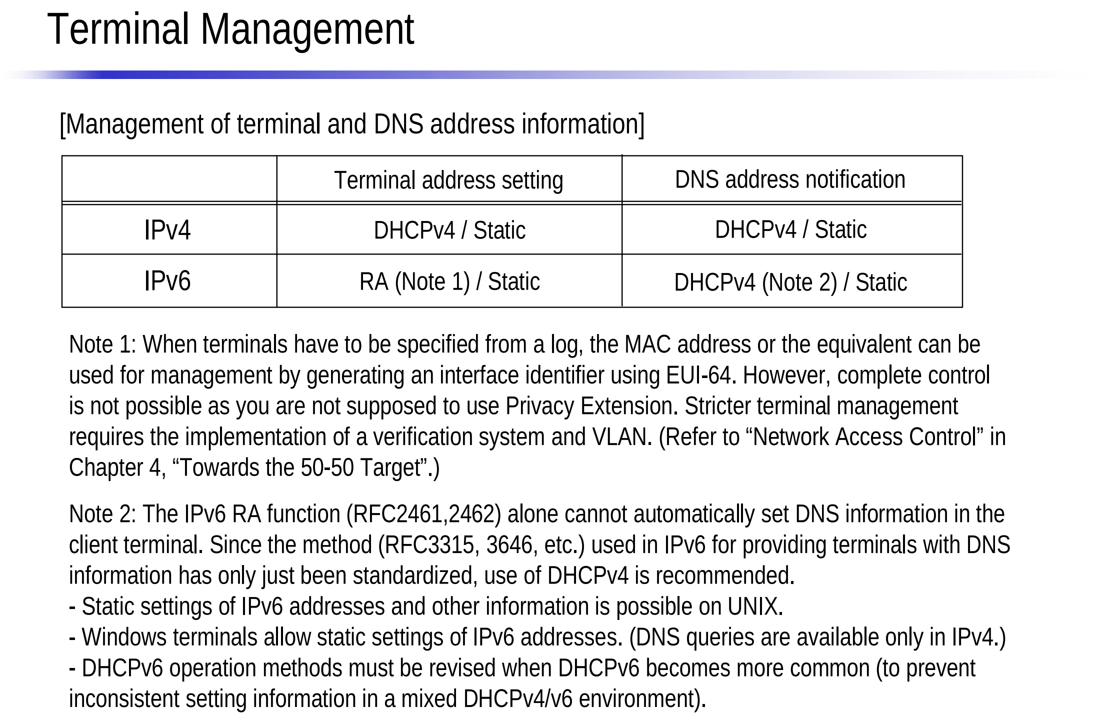
Note 1: Enables conversion of terminal equipment to IPv6 (This is not dependent on IP address, but requires verification from the service provider.)

Note 2: Not a service provided by current IPv6.

・In the initial stage of IPv6 tunneling will be used to provide IPv6 compatibility.
・A new service menu involving dual stack is being considered to handle high traffic loads.
・Line providers must be consulted regarding QoS maintenance and management of new IPv6 applications and existing IPv4 applications in the migration to IPv6.

Tunneling is the most realistic choice to convert to IPv6 at the initial stage. As loads increase a new service menu that includes a dual stack configuration should be installed. Consult your line providers regarding QoS maintenance and control of new IPv6 applications and existing IPv4 applications when IPv6 is deployed.

Terminal Management



Terminal Management

[Management of terminal and DNS address information]

	Terminal address setting	DNS address notification
IPv4	DHCPv4 / Static	DHCPv4 / Static
IPv6	RA (Note 1) / Static	DHCPv4 (Note 2) / Static

Note 1: When terminals have to be specified from a log, the MAC address or the equivalent can be used for management by generating an interface identifier using EUI-64. However, complete control is not possible as you are not supposed to use Privacy Extension. Stricter terminal management requires the implementation of a verification system and VLAN. (Refer to “Network Access Control” in Chapter 4, “Towards the 50-50 Target”.)

Note 2: The IPv6 RA function (RFC2461,2462) alone cannot automatically set DNS information in the client terminal. Since the method (RFC3315, 3646, etc.) used in IPv6 for providing terminals with DNS information has only just been standardized, use of DHCPv4 is recommended.
- Static settings of IPv6 addresses and other information is possible on UNIX.
- Windows terminals allow static settings of IPv6 addresses. (DNS queries are available only in IPv4.)
- DHCPv6 operation methods must be revised when DHCPv6 becomes more common (to prevent inconsistent setting information in a mixed DHCPv4/v6 environment).

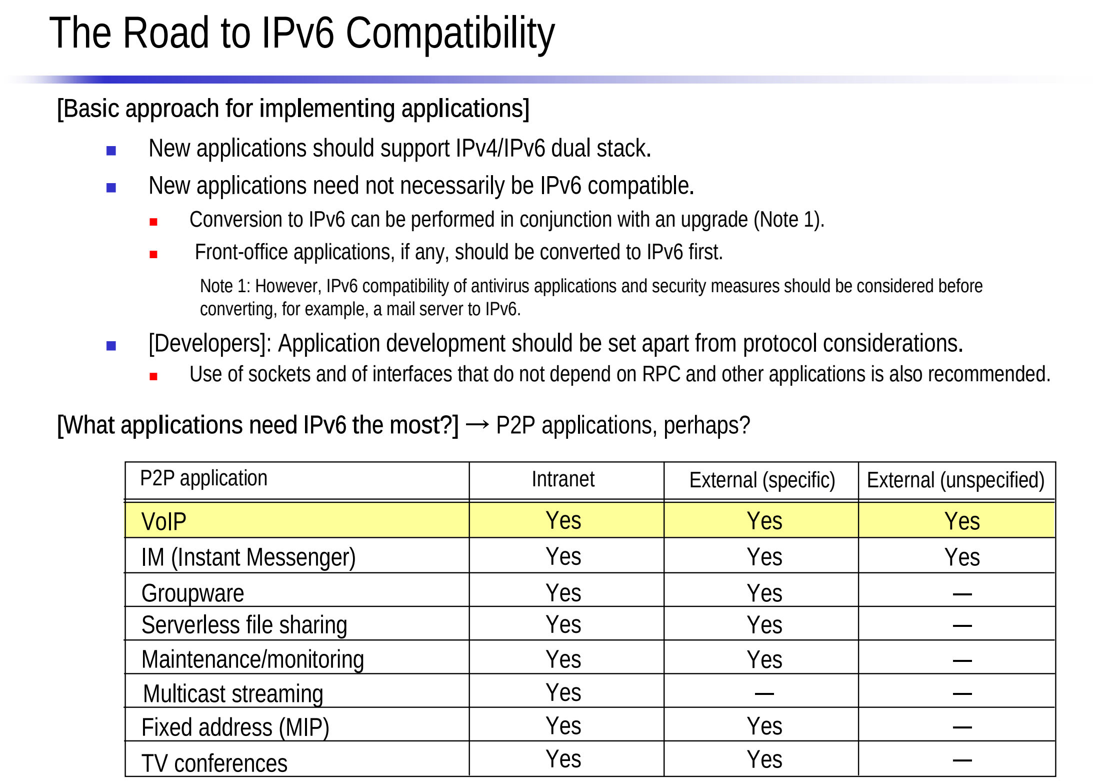
When terminals have to be specified from a log, the MAC address or the equivalent can be used for management by generating an interface identifier using EUI-64. Since independent interface identifiers can be set, complete control is not possible. Nor is Privacy Extension to be used. Stricter terminal management requires the implementation of a verification system and VLAN. (Refer to “Network Access Control” in Chapter 4, “Towards the 50-50 Target”.）

The RA function (RFC2461, 2462) alone cannot automatically set DNS information in the client terminal. Since the method (RFC3315, 3646, etc.) used in IPv6 for providing terminals with DNS information has only just been standardized, use of DHCPv4 is recommended.

- Static settings of IPv6 addresses and other information is possible on UNIX.
- Windows terminals allow static settings of IPv6 addresses. (DNS queries are available only in IPv4.)
- DHCPv6 operation methods must be revised when DHCPv6 becomes more common (to prevent inconsistent setting information in a mixed DHCPv4/v6 environment.)

5.3.6 Deploying IPv6 by Installing New IPv6 Compatible Applications

The Road to IPv6 Compatibility



The Road to IPv6 Compatibility

[Basic approach for implementing applications]

- New applications should support IPv4/IPv6 dual stack.
- New applications need not necessarily be IPv6 compatible.
  - Conversion to IPv6 can be performed in conjunction with an upgrade (Note 1).
  - Front-office applications, if any, should be converted to IPv6 first.

  Note 1: However, IPv6 compatibility of antivirus applications and security measures should be considered before converting, for example, a mail server to IPv6.
- [Developers]: Application development should be set apart from protocol considerations.
  - Use of sockets and of interfaces that do not depend on RPC and other applications is also recommended.

[What applications need IPv6 the most?] → P2P applications, perhaps?

P2P application	Intranet	External (specific)	External (unspecified)
VoIP	Yes	Yes	Yes
IM (Instant Messenger)	Yes	Yes	Yes
Groupware	Yes	Yes	—
Serverless file sharing	Yes	Yes	—
Maintenance/monitoring	Yes	Yes	—
Multicast streaming	Yes	—	—
Fixed address (MIP)	Yes	Yes	—
TV conferences	Yes	Yes	—

New applications should be IPv4/IPv6 dual stack compatible, but there is no need to rush to install IPv6 compatible versions of existing applications. Convert existing applications to IPv6 when the software is upgraded. Security measures must also be carefully considered before making a conversion, for example, in converting a mail server to IPv6, the virus checker must also be converted to IPv6. If any front-office applications are installed, they should be converted to IPv6 first (though there is no need to first convert internal networks to IPv6).

Application development should be considered separate from protocol dependency. Use of sockets and use of interfaces that do not depend on RPC or other applications is also recommended.

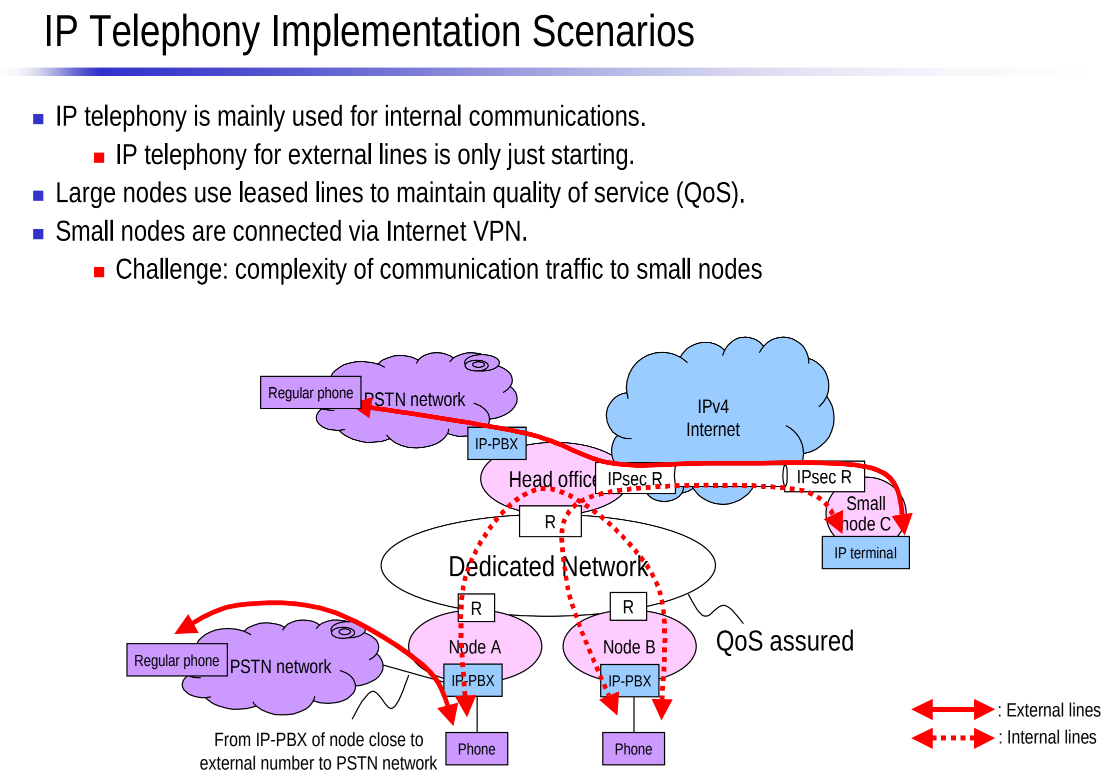
Applications suited to IPv6 are listed in the table above. P2P applications are perhaps in greatest need of IPv6.

VoIPv6 Solutions

Use of IP phones to cut down external connection costs is possible by subscribing to IPv6 and opening a port in the firewall for the required traffic. IPv6 telephony for external connections, which is now expected to take off, will be cheaper than an IPv4 external connection because of a lower load on external gateway (SIP-NAT) equipment, lower costs in obtaining global addresses and simplification of IP phones (calls do not converge on the center).

For the time being, security can be maintained by enabling only IPv6 telephony traffic through a firewall (by assigning a protocol ID or address). A full implementation will be performed according to the independent merging or staged replacement scenario depending on corporate security policy.

IP Telephony Implementation Scenarios



IP Telephony Implementation Scenarios

- IP telephony is mainly used for internal communications.
  - IP telephony for external lines is only just starting.
- Large nodes use leased lines to maintain quality of service (QoS).
- Small nodes are connected via Internet VPN.
  - Challenge: complexity of communication traffic to small nodes

This approach is not limited to IP telephony. When the load on a gateway becomes a performance bottleneck, IPv6 can be used as a “xx solution”

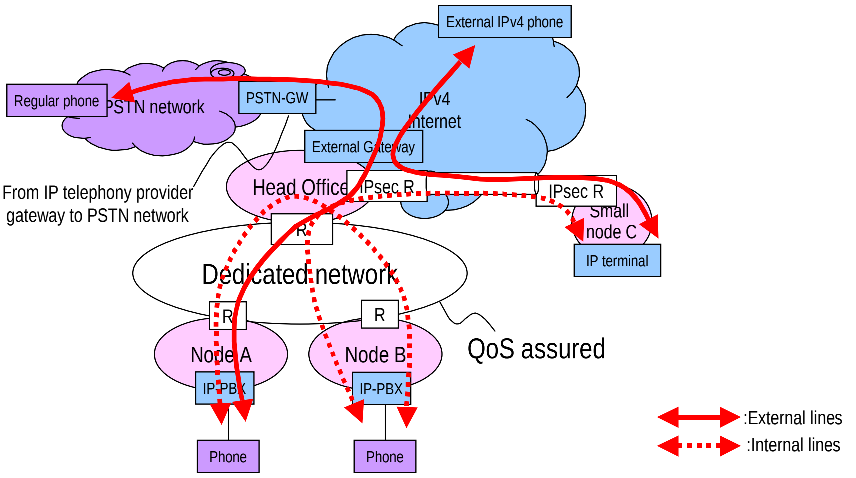
IP phones are currently mainly used for internal lines, but use over external lines will follow. An IPv4 solution in large nodes is to connect to leased lines to maintain QoS, while small nodes connect to Internet VPN. The drawback is that phone traffic routes for small nodes become needlessly complex.

Expansion of IP Telephony Through IPv4 (External Connection)

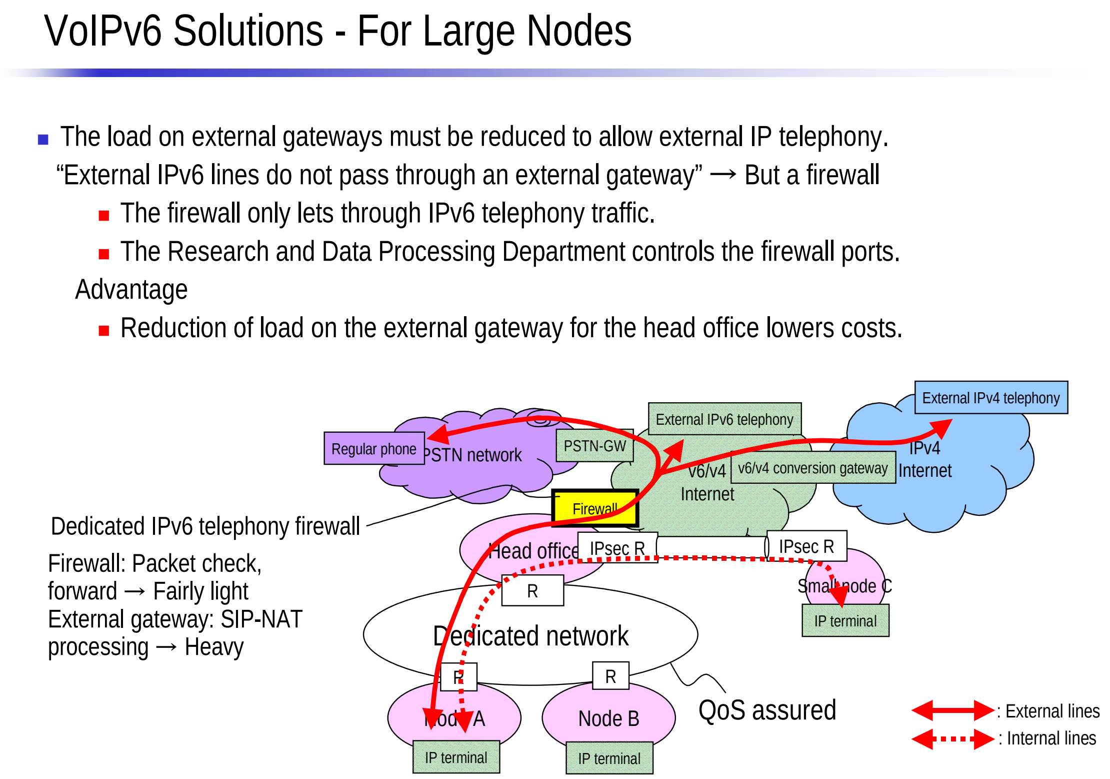
Expansion of IP Telephony Through IPv4 (External Connection)

- External gateways (SIP-NAT) are mandatory for connecting to external IP telephones.
- All external traffic are routed via external gateways (including PSTN calls).
- External gateways must have the capacity to satisfy demand.

→Costs increase to ensure speech quality



Use of IP phones via IPv4 requires an external gateway (SIP-NAT) to connect to an external IP phone. All external traffic goes via this external gateway (including PSTN calls). The capacity of the external gateway must be tailored to external line demands. Therefore ensuring good speech quality is a question of cost.



VoIPv6 Solutions - For Large Nodes

- The load on external gateways must be reduced to allow external IP telephony.
  “External IPv6 lines do not pass through an external gateway” → But a firewall
  - The firewall only lets through IPv6 telephony traffic.
  - The Research and Data Processing Department controls the firewall ports.

  Advantage
  - Reduction of load on the external gateway for the head office lowers costs.

Dedicated IPv6 telephony firewall

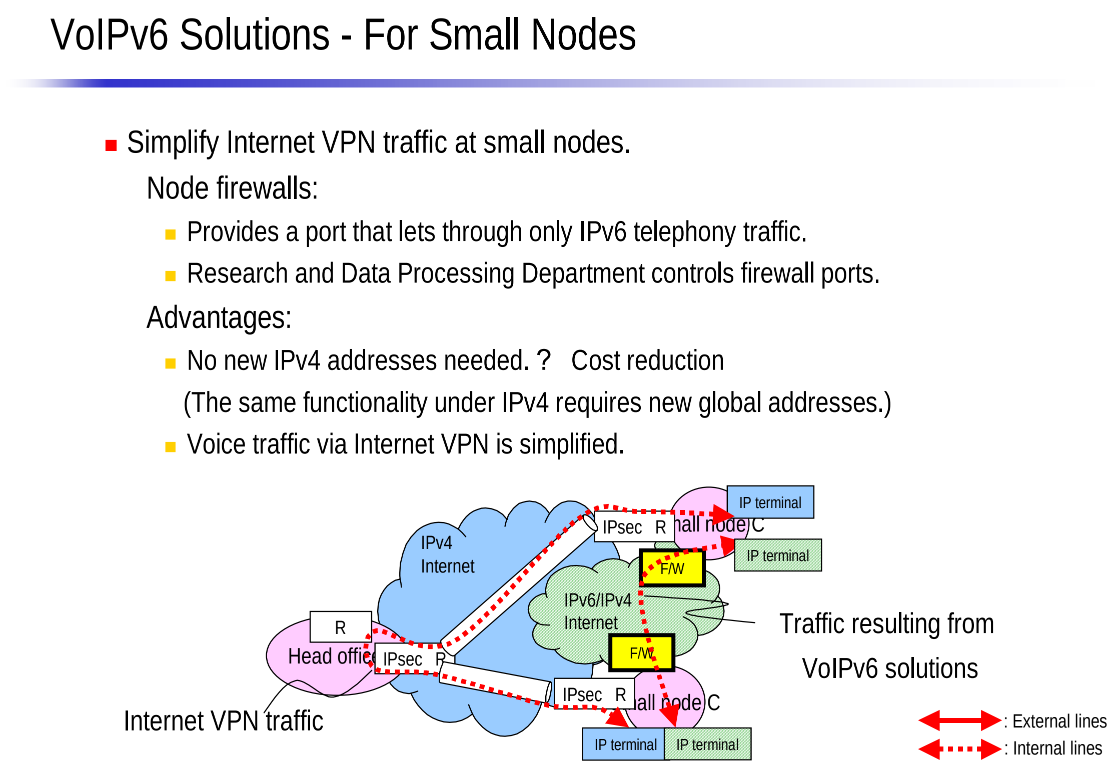
Firewall: Packet check, forward → Fairly light

External gateway: SIP-NAT processing → Heavy

For a large enterprise, implementing a VoIPv6 solution will reduce the load on the external gateway needed for making external IP phone connections. This is because external IPv6 lines do not go over the external gateway but through a firewall. Thus IPv6 telephony traffic will have to be assigned a port to reach the Internet. (The Research and Data Processing Department is in charge of firewall control.)

This reduces the load on the head office external gateway and lowers costs.

VoIPv6 Solutions - For Small Nodes



VoIPv6 Solutions - For Small Nodes

- Simplify Internet VPN traffic at small nodes.

  Node firewalls:
  - Provides a port that lets through only IPv6 telephony traffic.
  - Research and Data Processing Department controls firewall ports.

  Advantages:
  - No new IPv4 addresses needed. ? Cost reduction

    (The same functionality under IPv4 requires new global addresses.)
  - Voice traffic via Internet VPN is simplified.

The implementation of VoIPv6 will simplify Internet VPN traffic paths for small nodes.

Then the firewall of each node will provide a port to the Internet only for IPv6 telephony traffic. (The Research and Data Processing Department is in charge of firewall control.) The advantage of this arrangement is that no new IPv4 addresses will be needed which reduces costs (a similar configuration under IPv4 will require additional global addresses). Voice traffic paths via Internet VPN are also simplified.

VoIPv6 Solutions - Additional Advantages

The implementation of VoIPv6 has also other advantages.

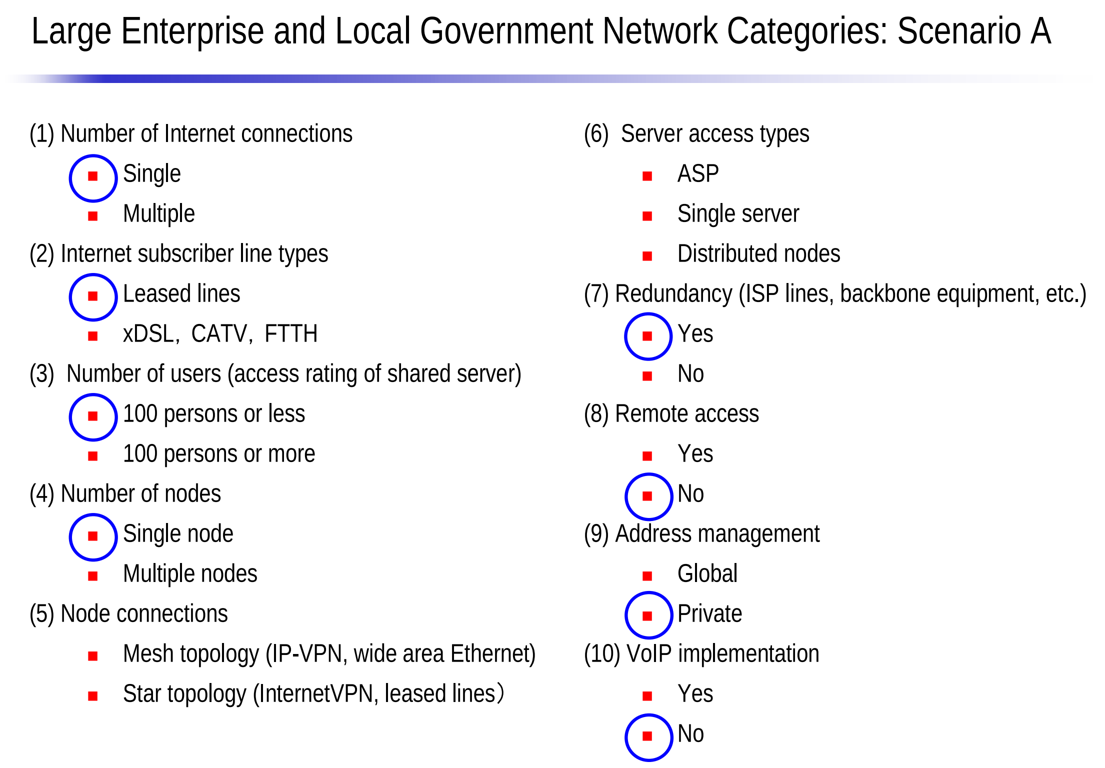
Growth in IP internal telephony will double the need for addresses. For example, in an office with 100 employees, servers, routers, printers and wireless applications (fixed assignment) will require 50 addresses, PCs (DHCP assignment) will require another 150. That is a total of 200 which can be handled by a /24 prefix. If 120 IP internal phones are added to this, a total of 320 addresses will be needed. This is more than a /24 prefix can handle. In IPv4, this would require changing the subnet mask or adding a separate segment (defining IP phones as a separate segment), in fact, making it necessary to redesign the subnet mask and thereby increasing design costs. In IPv6, these redesign costs (caused by adding terminals) are unnecessary.

5.3.7 Detailed IPv6 Deployment

The following introduces two IPv6 scenarios for two types of large enterprise and local government configurations.

Scenario A

Network Categories



Large Enterprise and Local Government Network Categories: Scenario A

(1) Number of Internet connections

- [✓ Single]
- Multiple

(2) Internet subscriber line types

- [✓ Leased lines]
- xDSL, CATV, FTTH

(3) Number of users (access rating of shared server)

- [✓ 100 persons or less]
- 100 persons or more

(4) Number of nodes

- [✓ Single node]
- Multiple nodes

(5) Node connections

- Mesh topology (IP-VPN, wide area Ethernet)
- Star topology (InternetVPN, leased lines）

(6) Server access types

- ASP
- Single server
- Distributed nodes

(7) Redundancy (ISP lines, backbone equipment, etc.)

- [✓ Yes]
- No

(8) Remote access

- Yes
- [✓ No]

(9) Address management

- Global
- [✓ Private]

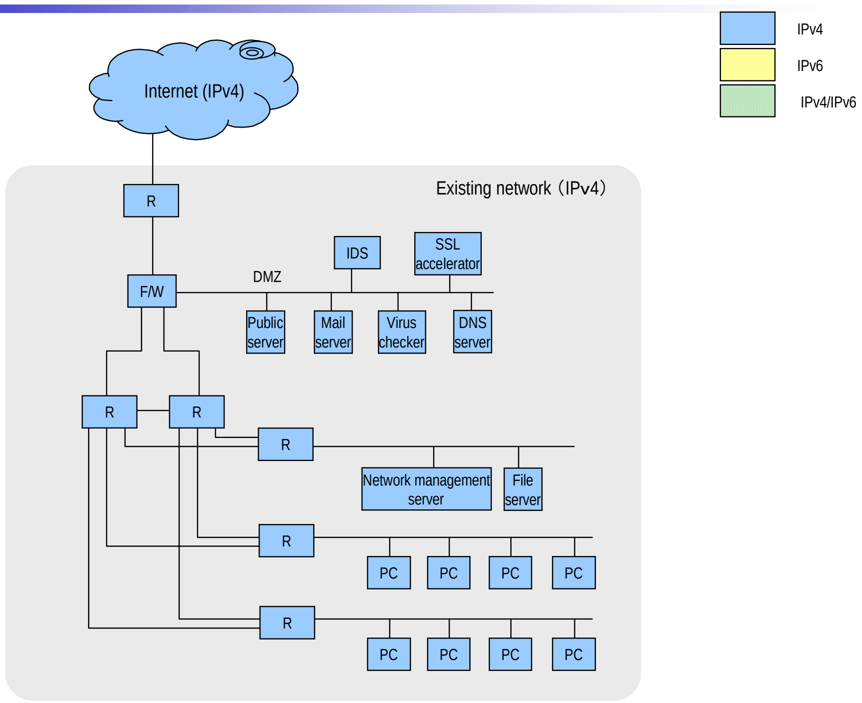
(10) VoIP implementation

- Yes
- [✓ No]

Scenario A leads to a comparatively small and simple network involving one node and 100 or fewer people. A leased line connects network to the Internet and there is no remote access or VoIP.

Network example

Large Enterprise and Local Government Network Example: Scenario A



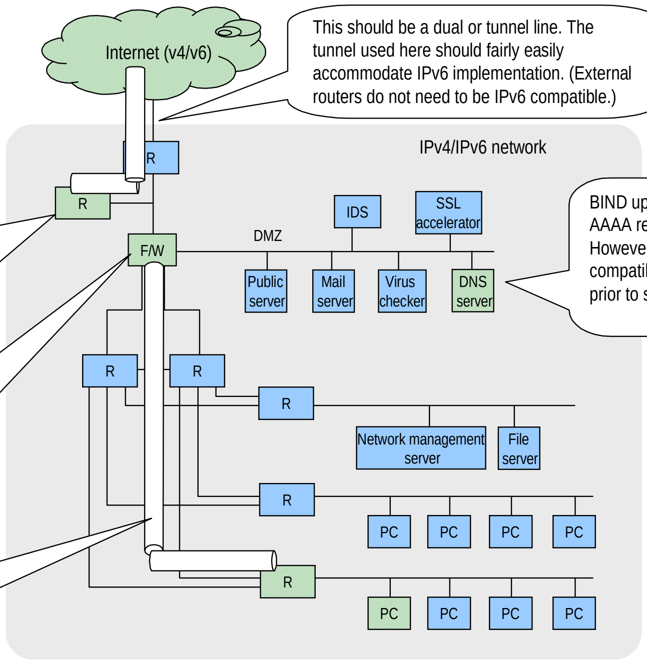
As shown in the figure, there is only a single connection to the Internet, and the Web server, the mail server and the DNS server are located in the DMZ.

Staged Replacement: Scenario A

🟦 IPv4
🟨 IPv6
🟩 IPv4/IPv6

[Step1]

(Currently feasible level)



This should be a dual or tunnel line. The tunnel used here should fairly easily accommodate IPv6 implementation. (External routers do not need to be IPv6 compatible.)

A separate IPv6 router can be installed to terminate tunnel. (It is also possible to terminate the tunnel with a firewall (external interface) or an external router supporting IPv6.)

BIND upgrade provides AAAA record support. However, check IPv6 compatibility of applications prior to storing AAAA records.

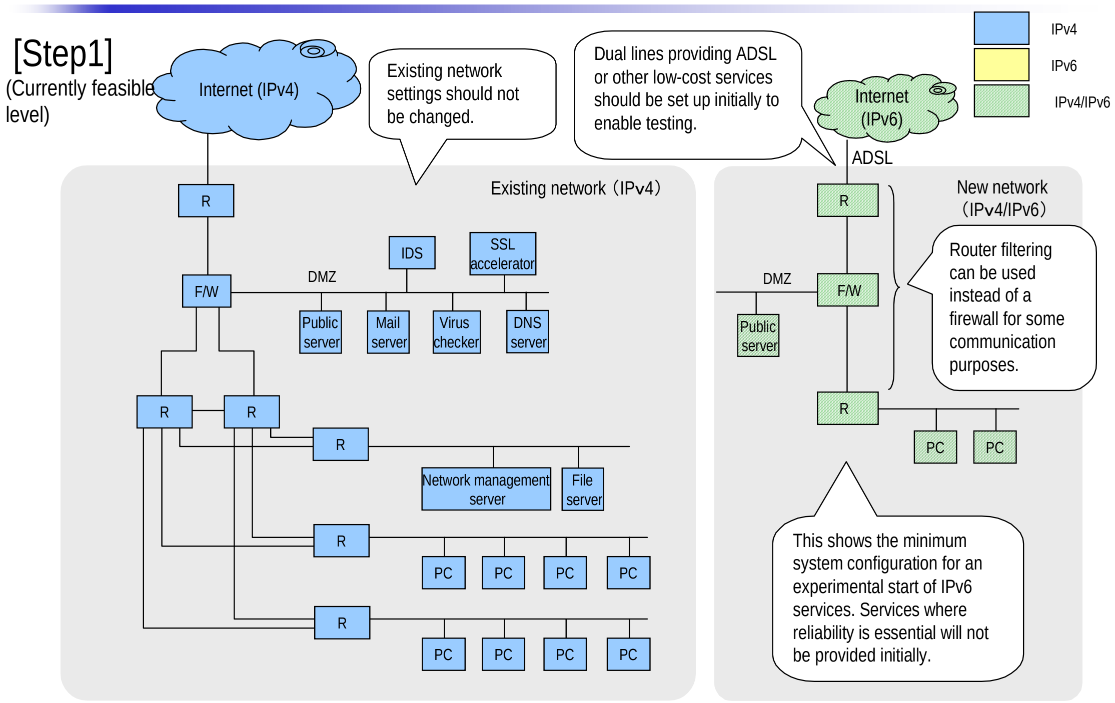
An IPv6 firewall must be set up. The bottom line is to maintain IPv4 management policies. The lowest minimum filtering conditions should be set for transfer of IPv6 packets.

To implement IPv6 service, tunneling should be tailored to the capacity of the internal network router to handle IPv6.

The above is a schematic representation of migration according to the staged replacement scenario. IPv6 connection is performed either by dual stack or tunnel. The figure shows a tunnel line, the simplest connection to make. A separate IPv6 router is connected to the end of the tunnel and an IPv6 firewall, which maintains a security policy similar to the IPv4 policy, is installed.

Migration by Independent Merging

Independent Merging: Scenario A



[Step1]
(Currently feasible level)

Existing network settings should not be changed.

Dual lines providing ADSL or other low-cost services should be set up initially to enable testing.

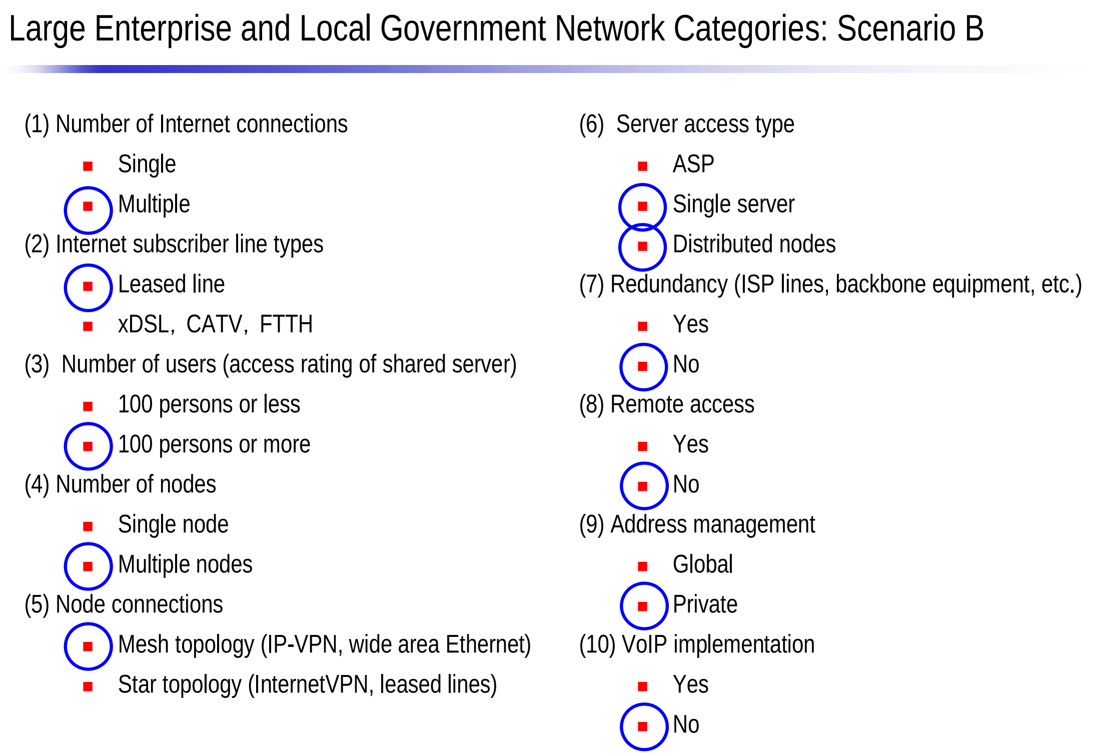
Router filtering can be used instead of a firewall for some communication purposes.

This shows the minimum system configuration for an experimental start of IPv6 services. Services where reliability is essential will not be provided initially.

In a migration with the independent merging scenario, a network with a separate IPv6 connection is built, but the existing network is left intact. Since the IPv6 network is implemented on an experimental basis, it is recommended that the minimum required system be built. For some systems router filter may replace the implementation of a firewall.

Scenario B

Large Enterprise and local government network categories



Large Enterprise and Local Government Network Categories: Scenario B

(1) Number of Internet connections

- Single
- [✓ Multiple]

(2) Internet subscriber line types

- [✓ Leased line]
- xDSL, CATV, FTTH

(3) Number of users (access rating of shared server)

- 100 persons or less
- [✓ 100 persons or more]

(4) Number of nodes

- Single node
- [✓ Multiple nodes]

(5) Node connections

- [✓ Mesh topology (IP-VPN, wide area Ethernet)]
- Star topology (InternetVPN, leased lines)

(6) Server access type

- ASP
- [✓ Single server]
- [✓ Distributed nodes]

(7) Redundancy (ISP lines, backbone equipment, etc.)

- Yes
- [✓ No]

(8) Remote access

- Yes
- [✓ No]

(9) Address management

- Global
- [✓ Private]

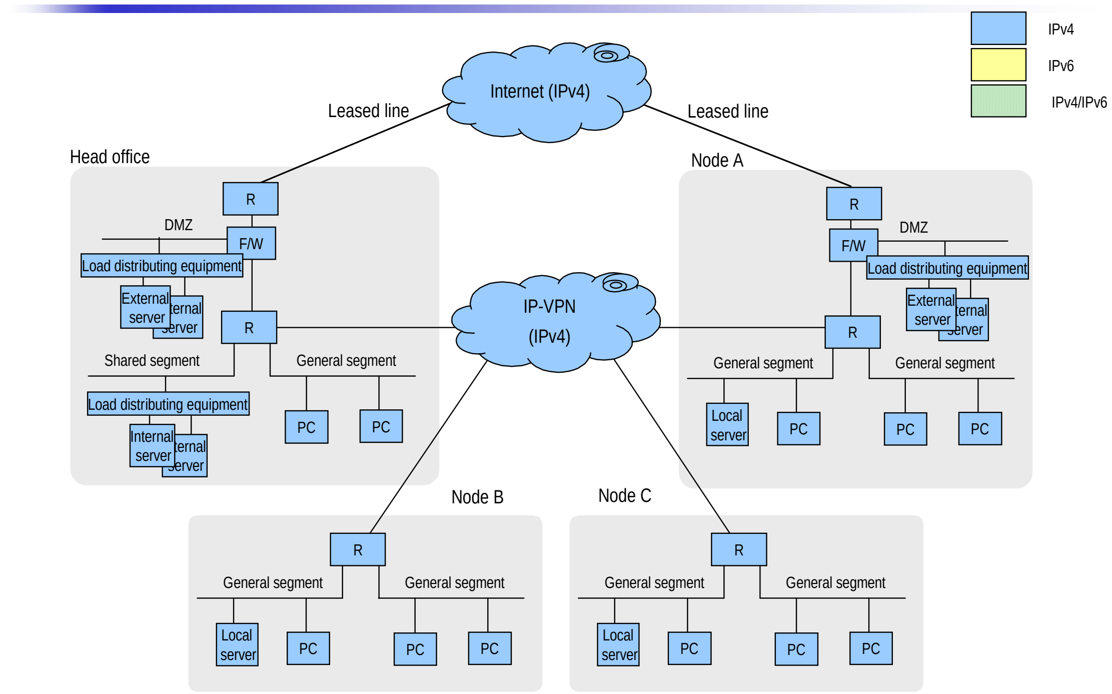
(10) VoIP implementation

- Yes
- [✓ No]

Scenario B is for a large enterprise or local government involving 100 people or more with multiple connections to the Internet.

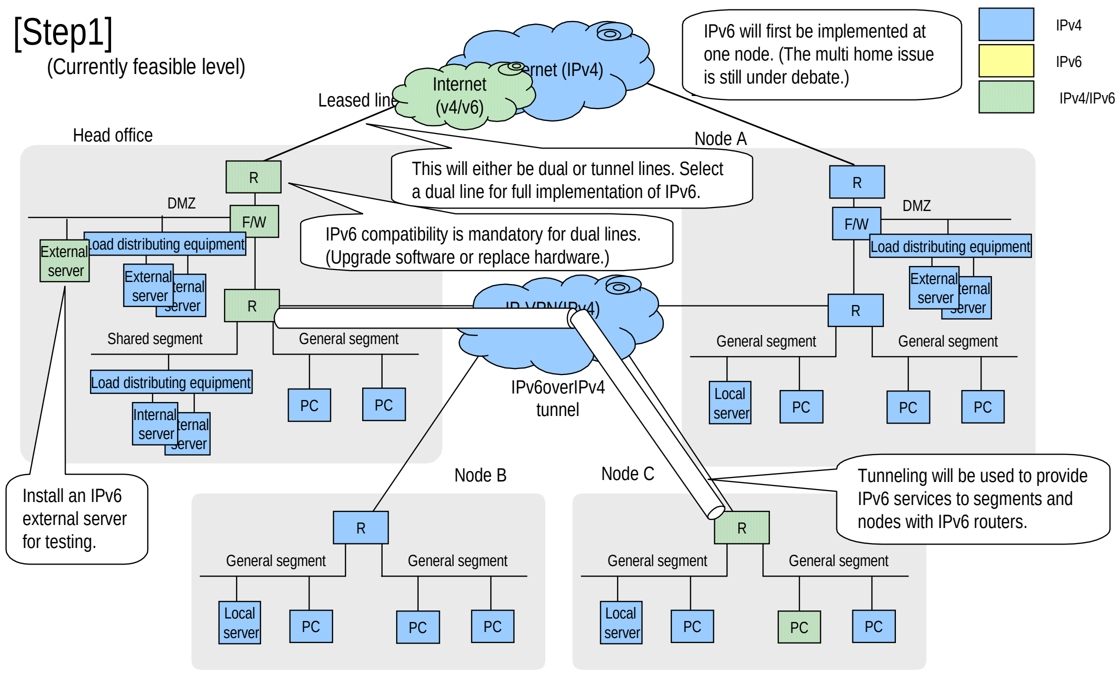
Network example

Large Enterprise and Local Government Network Example: Scenario B



Nodes are here connected according to a mesh topology.

Staged Replacement: Scenario B



[Step1]

(Currently feasible level)

IPv6 will first be implemented at one node. (The multi home issue is still under debate.)

This will either be dual or tunnel lines. Select a dual line for full implementation of IPv6.

IPv6 compatibility is mandatory for dual lines. (Upgrade software or replace hardware.)

Install an IPv6 external server for testing.

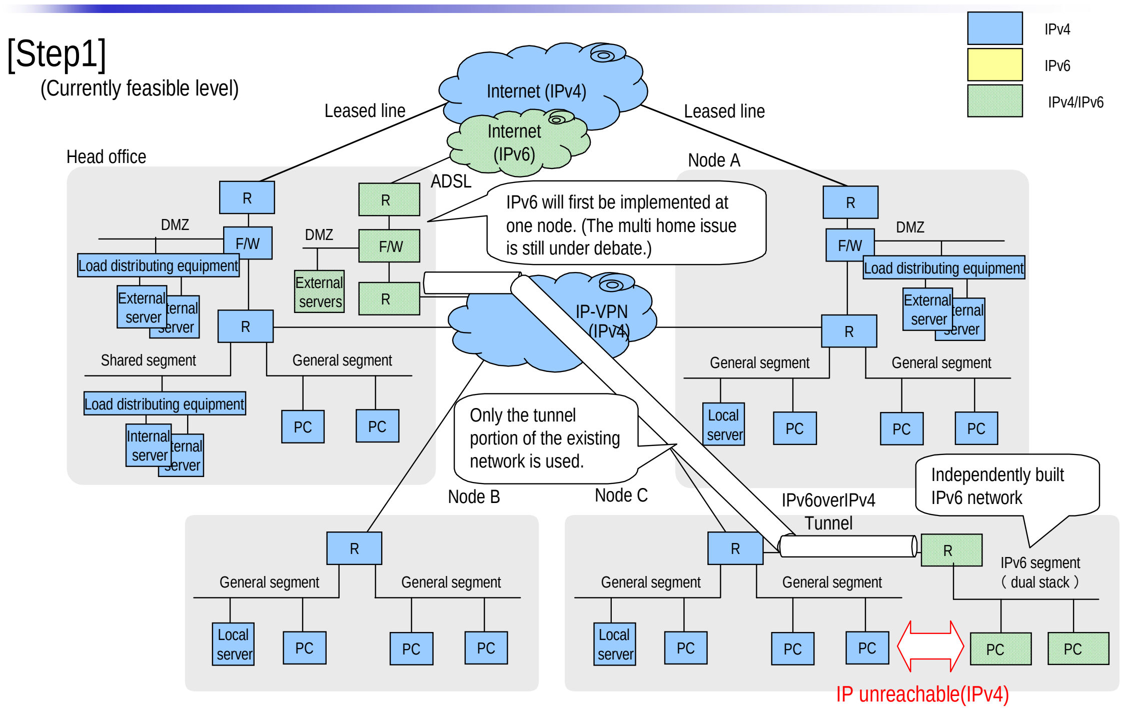
Tunneling will be used to provide IPv6 services to segments and nodes with IPv6 routers.

A schematic representation of staged replacement scenario B is shown above. An IPv6 connection could either be dual lines or tunnel lines. The head office of this company is connected to the Internet via dual lines, which offer the greatest potential for future full-scale implementation of IPv6. A dual line connection requires that IPv6 routers connect the network to the Internet. The IPv6 connection to the Internet is in this case restricted to one line. The reason for this is that multi homing in IPv6 is not yet a settled issue.

IPv6 over IPv4 tunneling is used to provide some nodes of this network with IPv6 connections.

Independent Merging migration

Independent Merging: Scenario B



[Step1]

(Currently feasible level)

IPv6 will first be implemented at one node. (The multi home issue is still under debate.)

Only the tunnel portion of the existing network is used.

Independently built IPv6 network

IP unreachable(IPv4)

Migration through independent merging is shown above. As shown, an IPv6 network that is fully independent of the existing network has been built. Separate nodes in the new network are connected via IPv6 over IPv4 tunneling and the nodes at both ends of the tunnel are separated from the existing network.

5.4 The 50-50 Target

5.4.1 IPv6 Environment and Basic Policies for a 50-50 Network

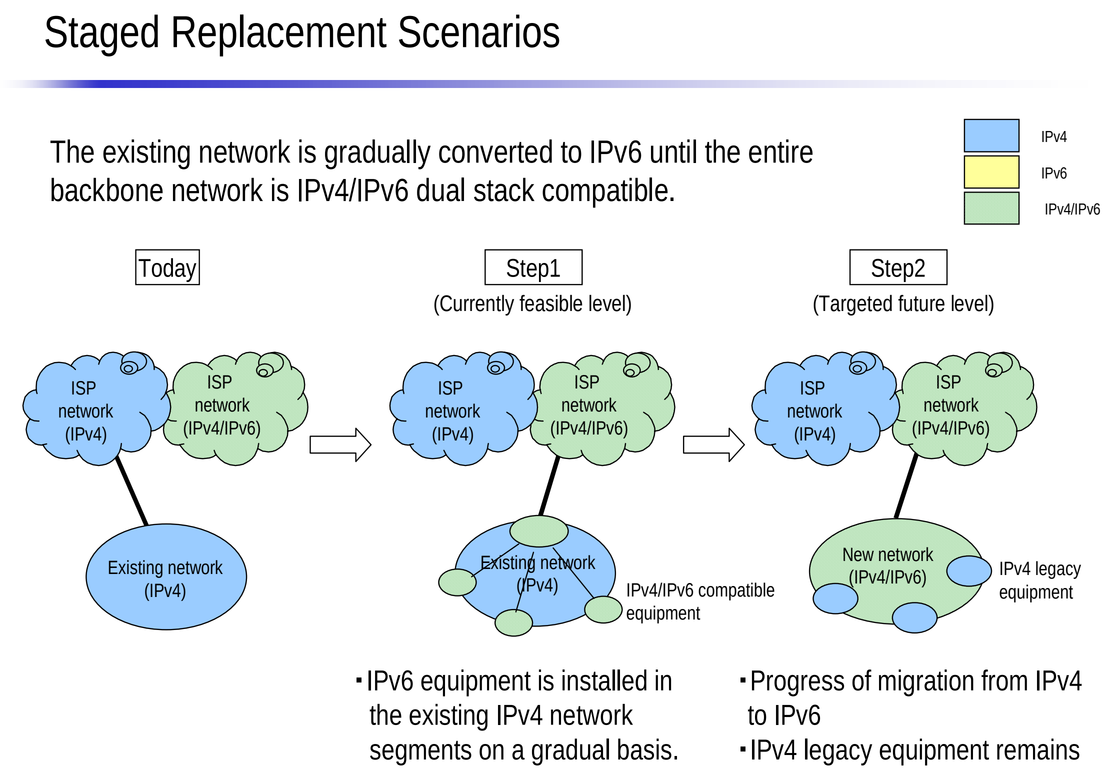
The IPv6 network environment will have reached a greater level of maturity when the IPv4-to-IPv6 ratio reaches the 50-50 mark. Small to medium-scale ISPs will then have started offering IPv6 line services (dual stack, tunnel connections) and a full line of IPv6 routers from large to small will be available. Operating systems will be providing full support for mobile, IPsec and other IPv6 functions. Also, use of various IPv6 application software programs will spread. Firewalls, IDS and similar security products in addition to a great number of other IPv6 applications will also be on offer.

When this watershed mark is reached, networks will have outgrown the framework originally set for them. For a start, non-PC networks and ubiquitous computing will have started to take off. Organization based security management is likely to have been replaced by security management handled by individuals representing a shift in human awareness. The accumulated amount of experience available then will have made possible the establishment of a security policy for IPv4/IPv6 dual environments. Thanks to this new security policy, applications that make full use of the potential of IPv6 will see the light of day accelerating the speed of migration from IPv4 to IPv6 networks. At the same time, intrusions and attacks using IPv6 and other cyber crime will start in earnest.

The basic policy will at this time be to move entire organizations to an IPv4/IPv6 dual stack network environment. Although there is no need to convert legacy applications to IPv6 en masse, now is the time to gradually move all applications into the IPv6 realm.

5.4.2 Staged Replacement

Migration scenarios



Staged Replacement Scenarios

The existing network is gradually converted to IPv6 until the entire backbone network is IPv4/IPv6 dual stack compatible.

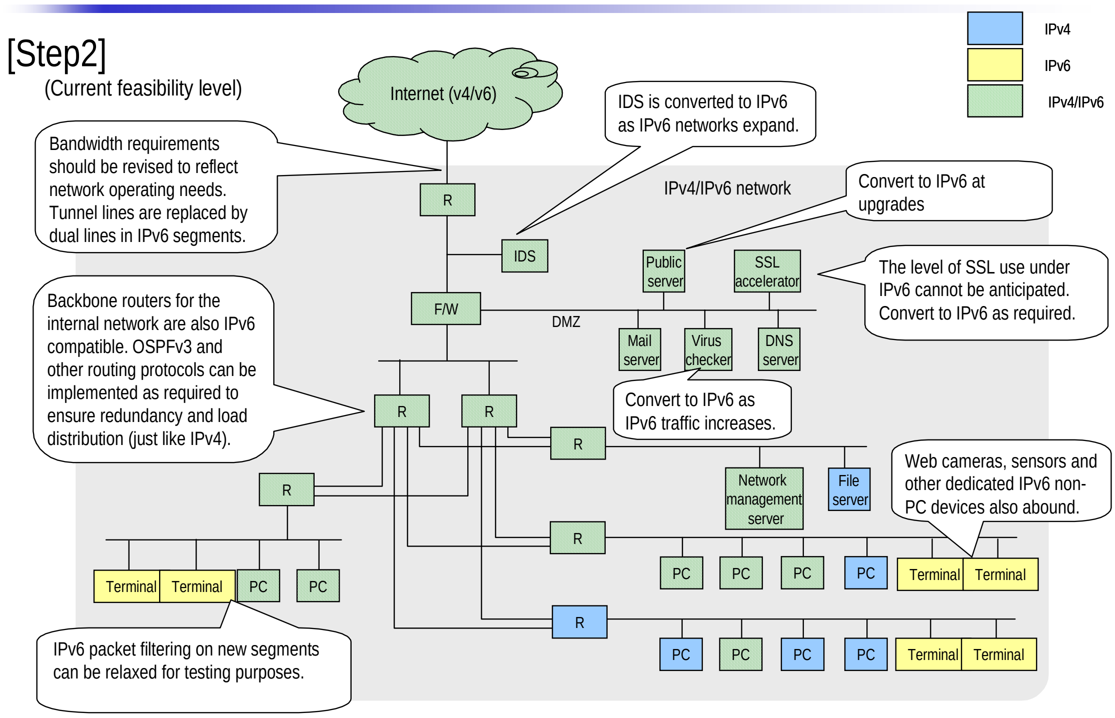
- IPv6 equipment is installed in the existing IPv4 network segments on a gradual basis.

- Progress of migration from IPv4 to IPv6
- IPv4 legacy equipment remains

A schematic overview of staged replacement is shown above. Part of the existing IPv4 network can be converted to an IPv4/IPv6 dual stack segment at the present stage. The next step will be to use IPv4/IPv6 dual stack terminals as the mainstay of the network leaving only a small segment of dedicated IPv4 terminals.

Scenario A

Staged Replacement: Scenario A



[Step2]

(Current feasibility level)

Bandwidth requirements should be revised to reflect network operating needs. Tunnel lines are replaced by dual lines in IPv6 segments.

Backbone routers for the internal network are also IPv6 compatible. OSPFv3 and other routing protocols can be implemented as required to ensure redundancy and load distribution (just like IPv4).

IPv6 packet filtering on new segments can be relaxed for testing purposes.

IDS is converted to IPv6 as IPv6 networks expand.

Convert to IPv6 at upgrades

The level of SSL use under IPv6 cannot be anticipated. Convert to IPv6 as required.

Convert to IPv6 as IPv6 traffic increases.

Web cameras, sensors and other dedicated IPv6 non-PC devices also abound.

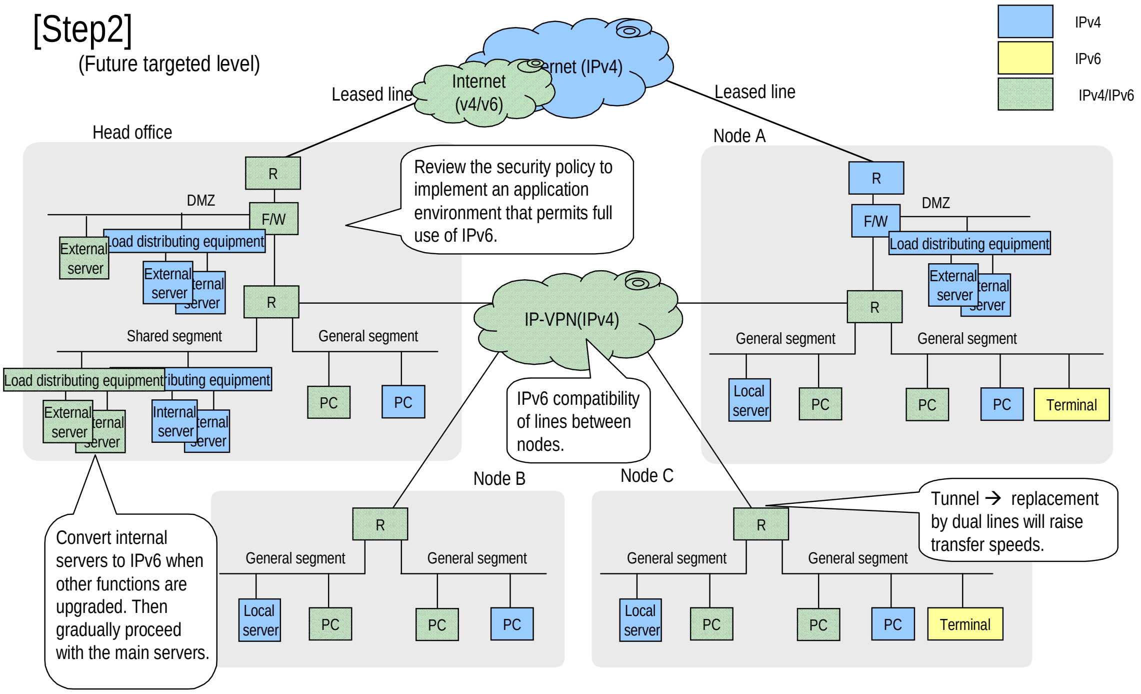
The figure above shows the development of large enterprise and local government networks that choose the staged replacement scenario A. Almost all internal terminals are dual stack terminals indicating that IPv6 is being used. Internet connections have been converted from tunnel to dual connections. A revision of network needs have ensured that connections of the right bandwidth is provided. Backbone routers have been replaced with IPv6 compatible products. OSPFv3 and other routing protocols have been installed to provide the same redundancy and load distribution as IPv4. IPv6 virus checkers and IDS products have been installed to handle the growing IPv6 traffic. It is not known to what extent SSL accelerators for public networks will be used in the IPv6 age, but these may also have to be converted to IPv6.

Scenario B

Staged Replacement: Scenario B

[Step2]

(Future targeted level)



Review the security policy to implement an application environment that permits full use of IPv6.

IPv6 compatibility of lines between nodes.

Tunnel → replacement by dual lines will raise transfer speeds.

Convert internal servers to IPv6 when other functions are upgraded. Then gradually proceed with the main servers.

Also in large enterprises and local governments that select scenario B aiming for a 50-50 environment, the majority of terminals in office nodes can communicate using IPv4 and IPv6. Expansion of functionality and upgrades have gradually brought in a dual stack internal server environment following a similar shift in external servers. Communications between nodes is also IPv6 compatible.

5.4.3 Migration Through Independent Merging

Migration scenario

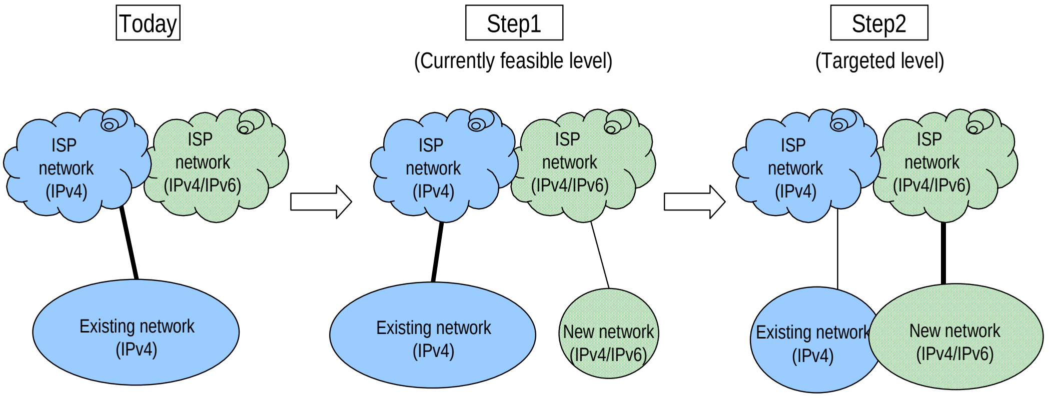
Independent Merging Migration Scenario

An independent IPv4/IPv6 dual stack network is merged with the existing network to enable a gradual migration.

🟦 IPv4

🟨 IPv6

🟩 IPv4/IPv6



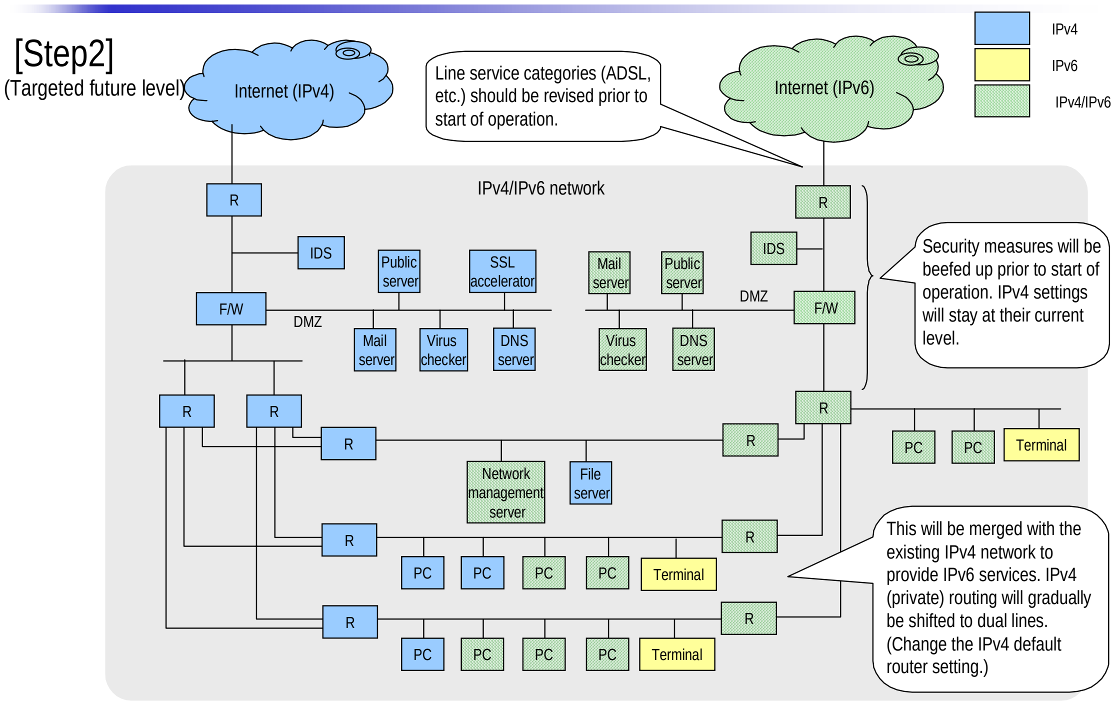
- An IPv4/IPv6 network is built independently of the existing IPv4 network.

- Fusion of existing IPv4 network and the new IPv4/IPv6 network
- Gradual migration to new IPv4/IPv6 network

In an independent merging scenario, an independent IPv4/IPv6 network will be built leaving the existing IPv4 network intact. Later the existing IPv4 network will be merged with the new IPv6 network and focus is gradually shifted to the new IPv4/IPv6 network.

Scenario A

Independent Merging: Scenario A



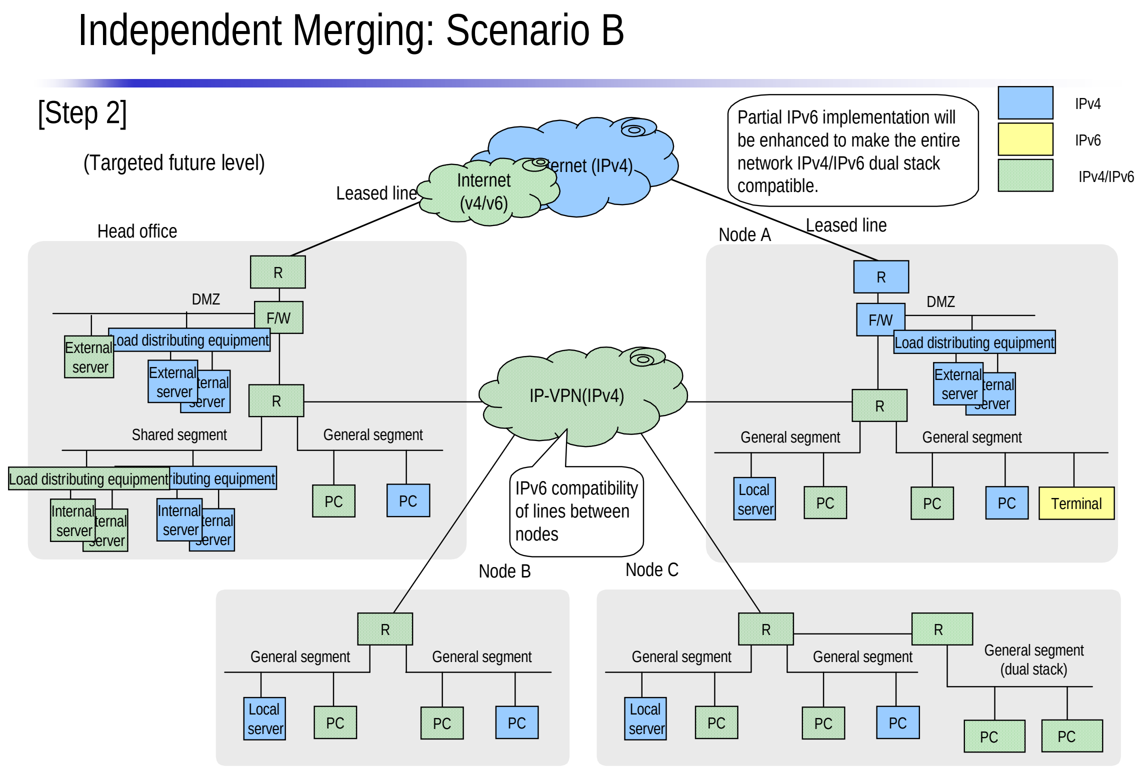
Line service categories (ADSL, etc.) should be revised prior to start of operation.

Security measures will be beefed up prior to start of operation. IPv4 settings will stay at their current level.

This will be merged with the existing IPv4 network to provide IPv6 services. IPv4 (private) routing will gradually be shifted to dual lines. (Change the IPv4 default router setting.)

So far the totally independent IPv4/IPv6 dual network in large enterprises and local governments that choose independent merging scenario A is merged with the existing IPv4 network. Then IPv4 routing in the existing network is switched to the dual line side and the IPv4 default router settings for terminals are changed. As the new network is merged with the IPv4 network, the security settings for the Internet connections on the dual line side ensure IPv4 level security.

Scenario B


Independent Merging: Scenario B

[Step 2]

(Targeted future level)

Partial IPv6 implementation will be enhanced to make the entire network IPv4/IPv6 dual stack compatible.

IPv6 compatibility of lines between nodes

The merging of the new network with the existing network in large enterprises and local governments selecting scenario B transforms the entire network to a dual stack network.

5.4.4 The Network Environment to Aim for in IPv6

An ideal network environment

An ideal large enterprise and local government network should offer plug and play as well as superior safety and ease of management.

End users should ideally be able to safely connect to the desired destination by just plugging in a terminal and without having to make any settings. Administrators should easily be able to identify the owner of the terminal and its location to enable centralized control.

Network topology

Although the topology will essentially remain the same as in IPv4, MobileIPv6 or similar technology look set to provide terminals with freedom of mobility.

Protocol stack

Dual stack networks will become the rule and dedicated IPv6 networks will, no doubt, appear. However, whether to select dual stack configuration servers or dedicated IPv6 servers depends on the cost of running both IPv4 and IPv6 stacks and the cost of IPv6 applications.

Security

For security reasons, a decision has to be made whether end-to-end communications should be available to all terminals or only to specific terminals. Another problem is whether encryption of end-to-end communications with external destinations should be allowed. This is related to the problem of whether administrators should be allowed to check communications as necessary.

Enabling IPv6 to live up to its full potential

Mobility is a topic that usually appears in discussions of how to fully use IPv6 in a large enterprise or a local government network. Dynamic name registration (via dynamic DNS or SIP perhaps) and Mobile IPv6 offer hope for the future. Another IPv6 only feature is end-to-end communications. This includes the following SIP-based communications: VoIP (internal and external), videoconferencing, file sharing, instant messaging, etc.

Methods for controlling access from other terminals

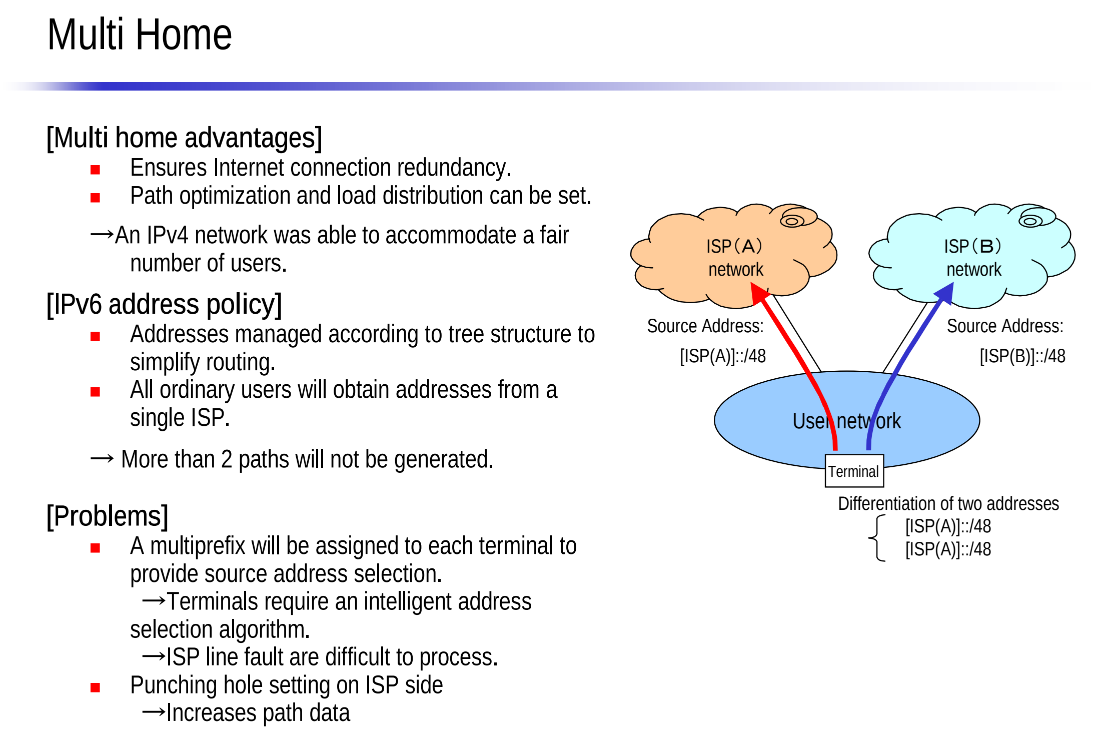
The method for controlling access between terminals must be modified to establish a network environment enabling end-to-end communications. The use of personal firewalls must be thoroughly debated. Functionality of IPsec and firewalls when regular employees access external destinations is also an important factor.

It should be determined whether access from outside the network in order to perform equipment maintenance should be made via Internet connections or over separate lines. Filtering by terminal routers, RA filtering by layer 2 switching, privacy extensions that enable use of random addresses for communications are some of the measures that should be considered to ensure internal access security and protect against source address spoofing attacks.

Each organization must settle what network services are to be allowed in the corporate network and their extent as well as the nature of network management and its scope.

5.5 Issues in Building a 50-50 Network

5.5.1 Multi Home



Multi Home

[Multi home advantages]

- Ensures Internet connection redundancy.
- Path optimization and load distribution can be set.

→An IPv4 network was able to accommodate a fair number of users.

[IPv6 address policy]

- Addresses managed according to tree structure to simplify routing.
- All ordinary users will obtain addresses from a single ISP.

→ More than 2 paths will not be generated.

[Problems]

- A multiprefix will be assigned to each terminal to provide source address selection.
  →Terminals require an intelligent address selection algorithm.
  →ISP line fault are difficult to process.
- Punching hole setting on ISP side
  →Increases path data

Multi home provides large enterprises and local governments with several important advantages, for example, redundancy in connections to the Internet, route optimization and load distribution.

Many users were able to get a foretaste of multi homing in IPv4. However, single user networks in IPv6 will not be provided with two or more routes. The IPv6 address policy uses a tree structure for address management to simplify routing and dictates that all ordinary users must obtain an address from an ISP.

However, IPv6 assigns addresses with multiple network prefixes for each terminal making it possible to set up application specific addresses. This is called Source Address Selection. To do this, terminals need an intelligent algorithm. Processing is impaired when faults occur in ISP lines.

Another approach is to set up a punching hole on the ISP side, which increases route data.

Multi home is an issue that must be solved to enable full use of an IPv6 network.

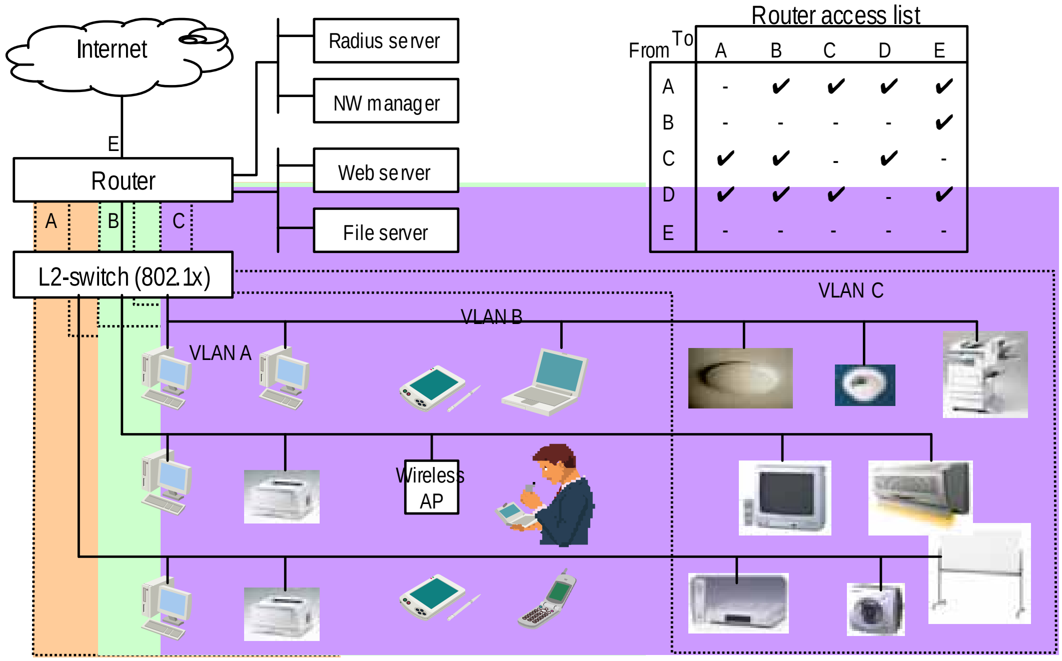
5.5.2 Network Access Control

A great variety of devices will be connected to an IPv6 network. This will include PCs and printers for the staff, non-staff member PCs and PDAs, whiteboards, cameras, illumination, air conditioners, sensors, monitor cameras, TVs, etc. All of these devices need not be managed at the same level. Thus network access should be controlled at a device specific level.

A solution would be to use VLAN to divide the network into a number of segments, use IEEE802.1x for verification and connect the devices to a specific segment. Separate access restrictions could be set up for each segment. A segment for staff PCs would allow all types of access, whereas another segment would be for guests accounts and only provide restricted access. Yet other segments for other devices would provide only internal access.

Network Access Control

[Schematic view of access control using IEEE802.1x and VLAN]



Router access list

From \ To	A	B	C	D	E
A	-	✔	✔	✔	✔
B	-	-	-	-	✔
C	✔	✔	-	✔	-
D	✔	✔	✔	-	✔
E	-	-	-	-	-

Originally a wired network technology, 802.1x is increasingly being used for user verification in wireless LAN networks. This technology could also be applied to different VLANs to create separate security zones for PCs and non-PCs depending objective and application.

5.5.3 Other Issues in Building a 50-50 Network (Non-Security Issues)

Another problem is the renumbering of addresses when ISP subscriptions are converted from IPv4 to IPv4/IPv6 dual stack networks and major external lines are changed from the existing network to the new network lines. The time and effort to effect this change should be kept to a minimum.

In addition to ISPs, IDCs, wholesalers and other agencies must become IPv6 compatible.

The following applications have problems that require a solution.

DNS

DNS discovery, DNS registration methods, new naming methods

Mail, Web

IPv6 compatible virus checkers and content checkers

Group ware

Special client software (including Web services), use of server IPv6 technology (reverse proxy, translators, etc.)

File sharing

Naming, signaling, security

Marketplace

For all types of software

5.6 Security Model

5.6.1 Basic Security Policies

In what way do IPv6 and IPv4 security policies differ? Like IPv4, IPsec is included in IPv6 as standard. Better security measures are necessary for both IPv4 and IPv6 in the following respects.

- Prevention of unauthorized access (firewall, IDS, etc.)
- Prevention of data leaks (encryption, passwords and other settings (individual management), etc.)
- Anti-virus measures (anti-virus applications, etc.)

However, with the change from IPv4 to IPv6, and the introduction of new applications (such as P2P communication, real-time and wide band services, etc.) there is an urgent need for a new security policy.

An IPv6 security model and many of the products and solutions for making it happen are not yet available. A temporary solution will have to be applied in the meantime to gradually improve network security.

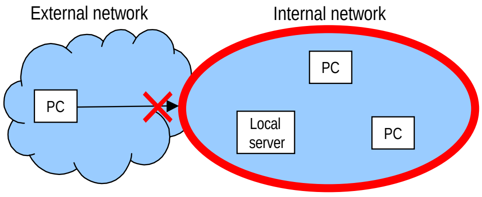
5.6.2 Gate Model and Safety Box Model

Gate Model and Safety Box Model

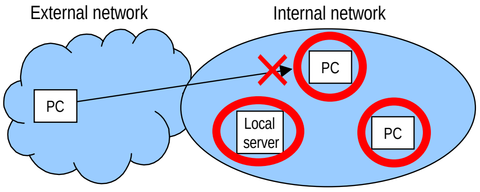
Convenience and security are often conflicting goals.

- Gate model
  - A feeling of security
  - A feeling that things are being ably managed
  - Vulnerable to crime inside the gate
- Safety box model
  - A feeling of insecurity
  - Complete assurance is currently not possible.
  - Flexible (remote access)

→ Security management will for the time being be based on the gate model. A hybrid model that combines the best features of both is likely to become the future model of choice.



Gate model



Safety box model

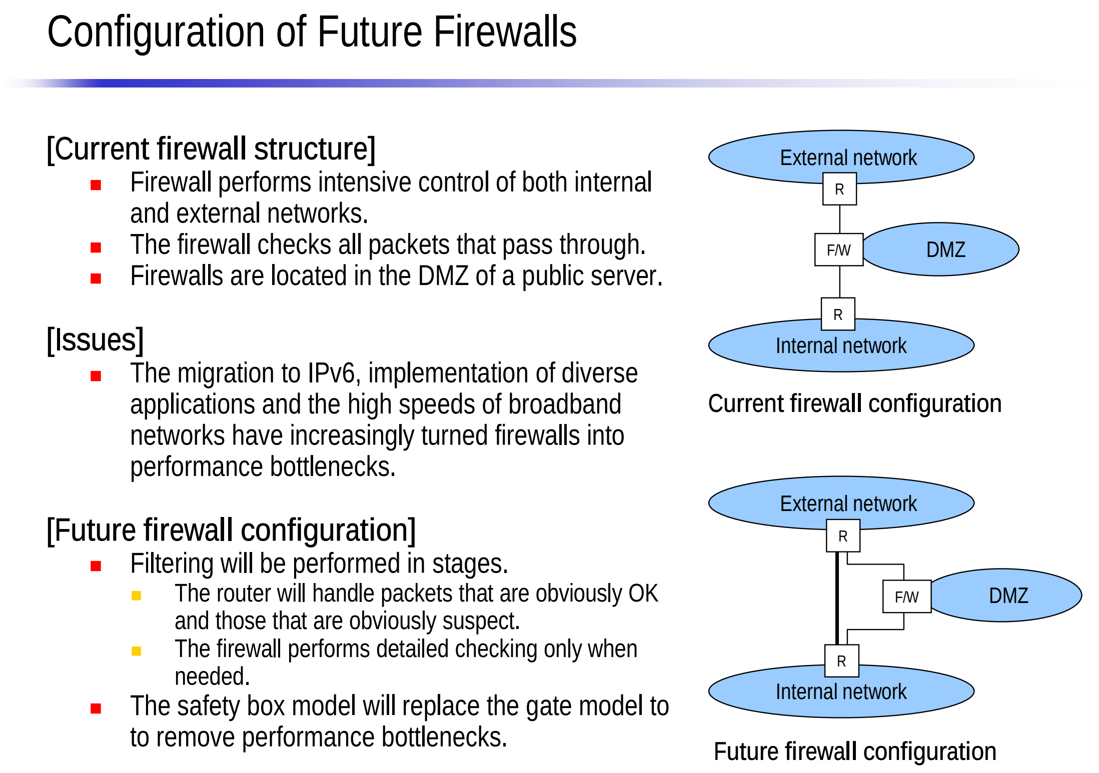
Convenience and security are often conflicting goals.

The gate model, which encloses the private network and protects if from the public network, is the current mainstream network security model. It gives its users peace of mind and a feeling that things are managed on their behalf. However, the deployment of broadband networks means that this model may become a performance bottleneck. It is also vulnerable to crime inside the boundary.

The safety box model in which each terminal and device connected to the network manages its own security does not inspire confidence and is difficult manage, but offers greater flexibility, for example, by offering remote access.

The gate model is likely to remain the major security management model for some time to come. In future, a hybrid model that combines the best features of both models is likely to replace them.

5.6.3 Configuration of Future Firewalls



Configuration of Future Firewalls

[Current firewall structure]

- Firewall performs intensive control of both internal and external networks.
- The firewall checks all packets that pass through.
- Firewalls are located in the DMZ of a public server.

[Issues]

- The migration to IPv6, implementation of diverse applications and the high speeds of broadband networks have increasingly turned firewalls into performance bottlenecks.

[Future firewall configuration]

- Filtering will be performed in stages.
  - The router will handle packets that are obviously OK and those that are obviously suspect.
  - The firewall performs detailed checking only when needed.
- The safety box model will replace the gate model to to remove performance bottlenecks.

Current firewall configuration

Future firewall configuration

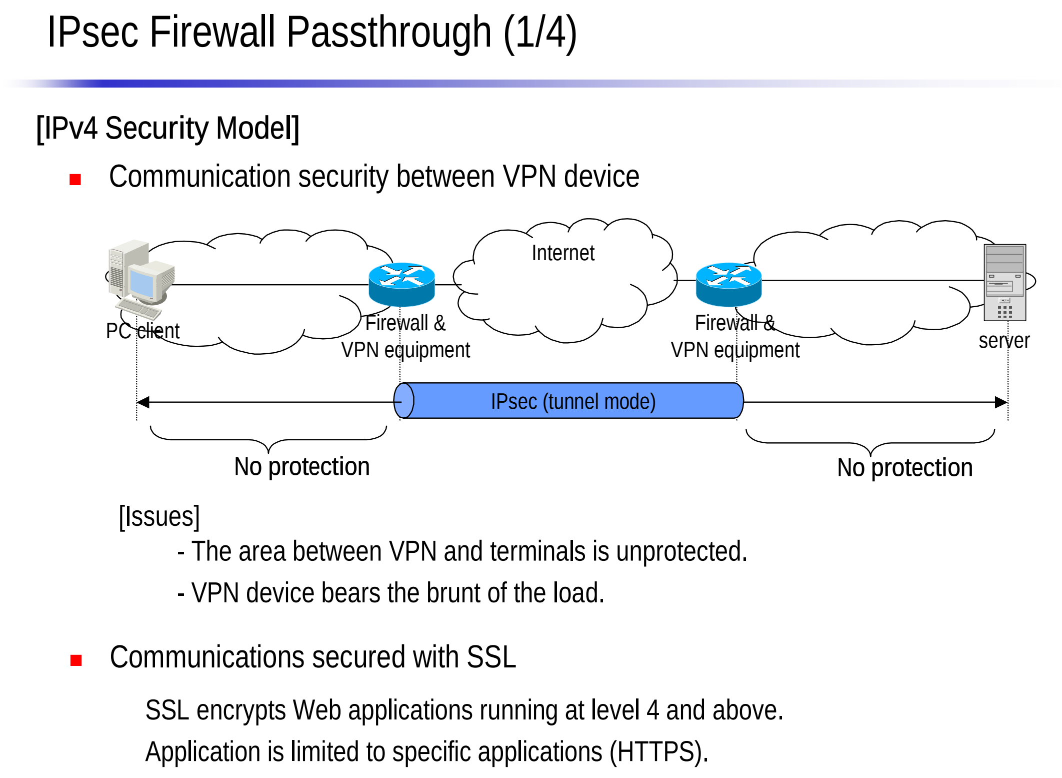
A firewall controls access between an external and internal network and checks each packet before letting it through. A public server is a server located in a DMZ, which is located in a segment separated from the internal network.

The problems is that with the introduction of IPv6, a great number of new applications as well as the higher speed of broadband connections, this type of firewall is a waste of bandwidth. A conventional firewall cannot handle the challenges of the new network in an efficient manner.

In future firewalls, filter processing will be split up between different entities. Routers will process packets that are obviously OK and those that are obviously suspect. The firewall will go into action only when a detailed check is called for. And a move from the gate model to the safety box model will also remove a performance bottleneck.

5.6.4 IPsec Firewall Passthrough

IPv4 Security Model



IPsec Firewall Passthrough (1/4)

[IPv4 Security Model]

- Communication security between VPN device

[Issues]

- The area between VPN and terminals is unprotected.

- VPN device bears the brunt of the load.

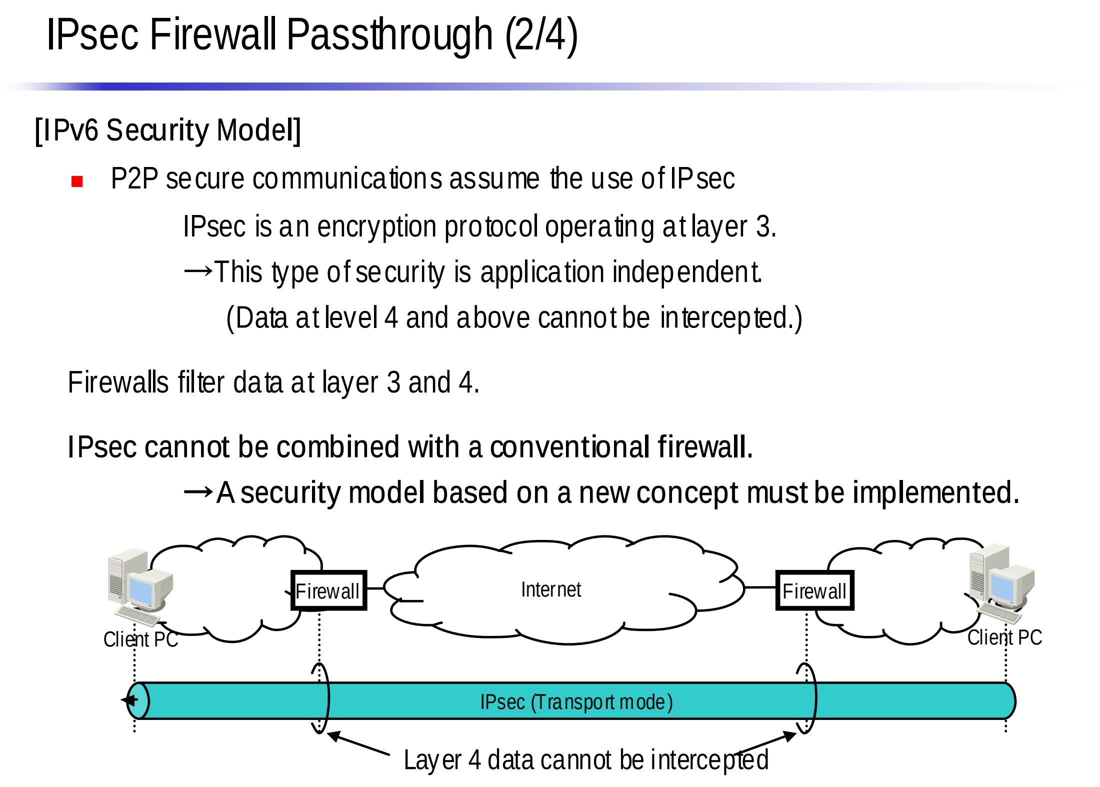
- Communications secured with SSL

SSL encrypts Web applications running at level 4 and above.

Application is limited to specific applications (HTTPS).

At present, security control is concentrated on the segment between VPN devices. The problem with this is that the segment between VPN devices and the terminals is not protected and that the processing load is concentrated on VPN devices. Another problem is that SSL is often used to secure communications although SSL handles encryption of Web applications at layer 4 and above and can only be applied to specific applications (HTTPS).

IPv6 Security Model



IPsec Firewall Passthrough (2/4)

[IPv6 Security Model]

- P2P secure communications assume the use of IPsec

  IPsec is an encryption protocol operating at layer 3.

  →This type of security is application independent.

  (Data at level 4 and above cannot be intercepted.)

Firewalls filter data at layer 3 and 4.

IPsec cannot be combined with a conventional firewall.

→A security model based on a new concept must be implemented.

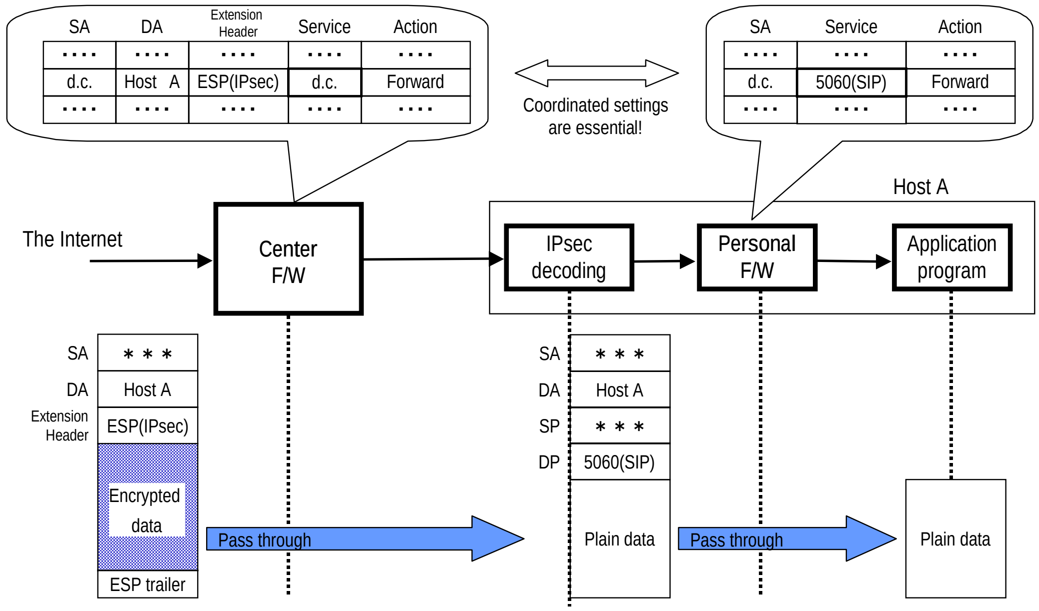
In the IPv6 security model, IPsec is more often used at the terminal level. IPsec is an encryption protocol operating in layer 3 that is not application dependent (but cannot reference data at layer 4 or above).

The firewall performs filtering on the basis of information provided by 3 and 4. Thus IPsec and firewalls must be able to coexist and this requires a security model based on a new concept.

Coordinating Filtering Between Personal and Center Firewalls

IPsec Firewall Passthrough (3/4)

[Example of Solutions]: Coordinating Filtering between Personal and Center Firewalls



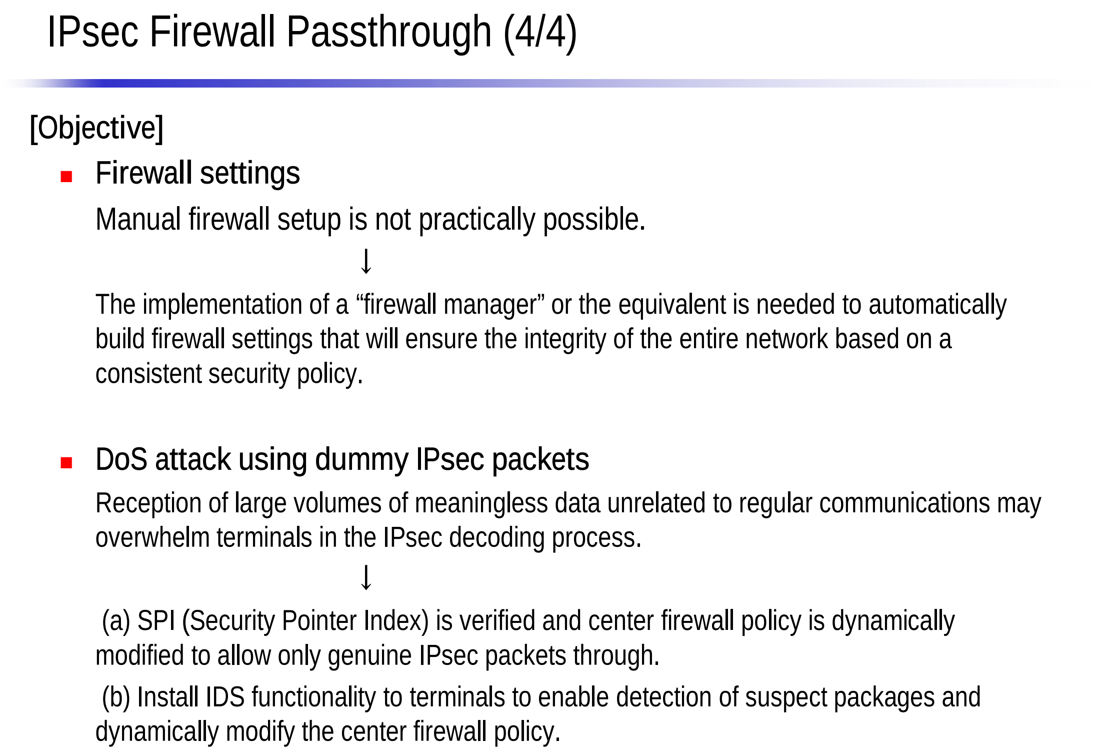
SA	DA	Extension Header	Service	Action
····	····	····	····	····
d.c.	Host A	ESP(IPsec)	d.c.	Forward
····	····	····	····	····

Coordinated settings are essential!

SA	Service	Action
····	····	····
d.c.	5060(SIP)	Forward
····	····	····

As shown in the figure, this can be solved by coordinating the filtering that is performed by the personal firewall and that performed by the center firewall. Thus if the center firewall lets through an IPsec communication between two terminals, the personal firewall filters the packet after decoding it.

Issues



IPsec Firewall Passthrough (4/4)

[Objective]

- Firewall settings

  Manual firewall setup is not practically possible.

  ↓

  The implementation of a "firewall manager" or the equivalent is needed to automatically build firewall settings that will ensure the integrity of the entire network based on a consistent security policy.

- DoS attack using dummy IPsec packets

  Reception of large volumes of meaningless data unrelated to regular communications may overwhelm terminals in the IPsec decoding process.

  ↓

  (a) SPI (Security Pointer Index) is verified and center firewall policy is dynamically modified to allow only genuine IPsec packets through.

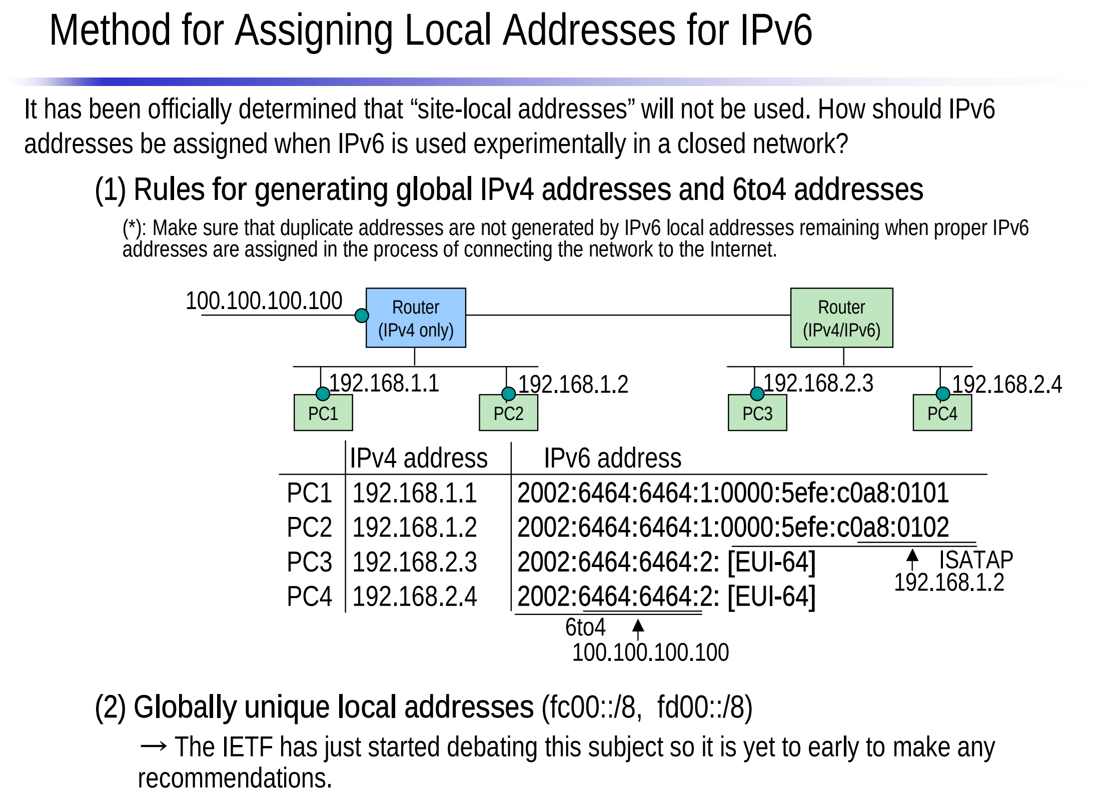
  (b) Install IDS functionality to terminals to enable detection of suspect packages and dynamically modify the center firewall policy.

Opening the firewall for IPsec communications must be carefully managed depending on the requirements of IPsec. However, it is not possible to handle the settings of each firewall manually. Consequently, a firewall manager or similar function that automatically manages firewall settings according to a consistent security policy and coordinates firewall operation is required.

The new process must also be capable of handling a DoS attack using dummy IPsec packets since the risk of the new process is that terminals could be overwhelmed by the decoding of a huge number of meaningless IPsec packets that are not part of an actual message. This can be prevented by checking the (a) SPI (Security Pointer Index) and dynamically change the center firewall policy accordingly to let through only genuine IPsec packets. And also by (b) installing an IDS function in each terminal that dynamically changes center firewall policy when a suspect packet is detected.

5.7 Tips & Tricks

5.7.1 Method for Assigning Local Addresses for IPv6



Method for Assigning Local Addresses for IPv6

It has been officially determined that “site-local addresses” will not be used. How should IPv6 addresses be assigned when IPv6 is used experimentally in a closed network?

(1) Rules for generating global IPv4 addresses and 6to4 addresses

(*): Make sure that duplicate addresses are not generated by IPv6 local addresses remaining when proper IPv6 addresses are assigned in the process of connecting the network to the Internet.

100.100.100.100

Router (IPv4 only)

Router (IPv4/IPv6)

192.168.1.1 PC1

192.168.1.2 PC2

192.168.2.3 PC3

192.168.2.4 PC4

	IPv4 address	IPv6 address
PC1	192.168.1.1	2002:6464:6464:1:0000:5efe:c0a8:0101
PC2	192.168.1.2	2002:6464:6464:1:0000:5efe:c0a8:0102
PC3	192.168.2.3	2002:6464:6464:2: [EUI-64]
PC4	192.168.2.4	2002:6464:6464:2: [EUI-64]

ISATAP 192.168.1.2

6to4 100.100.100.100

(2) Globally unique local addresses (fc00::/8, fd00::/8)

→ The IETF has just started debating this subject so it is yet to early to make any recommendations.

It is officially determined that “site-local addresses” for private networks will not be used in IPv6. How is it then possible to assign IPv6 addresses when deploying IPv6 in a closed network for experimental purposes? Two methods for solving this problem are described below.

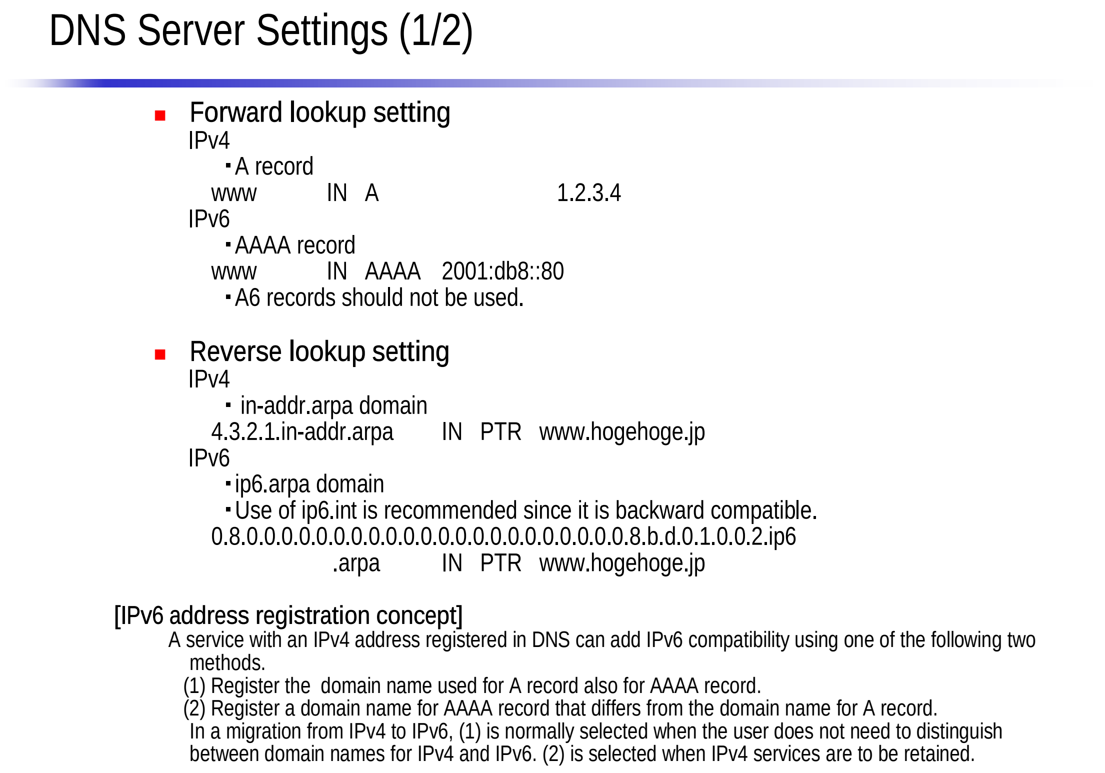
Rule for generating global IPv4 addresses and 6to4 addresses

This rule prevents the generation of duplicate addresses by any remaining IPv6 local addresses when a network is connected to the Internet after obtaining officially recognized IPv6 addresses. In 6to4, the hexadecimal representation of 2002:: and the 6to4 relay router IPv4 address is used as the network prefix. As shown in the figure below, the router IPv4 address is used to implement communications between IPv4/IPv6 dual stack terminals in an organization below 6to4 router addressing.

Globally unique local addresses (fc00::/8, fd00::/8)

Globally unit local addresses are used instead of site-local addresses to assign unique private network addresses. However, this solution is still being debated by the IETF and its use is therefore not recommended.

5.7.2 DNS Server Settings



DNS Server Settings (1/2)

- Forward lookup setting

IPv4

・A record

```
www        IN   A              1.2.3.4
```

IPv6

・AAAA record

```
www        IN   AAAA   2001:db8::80
```

・A6 records should not be used.

- Reverse lookup setting

IPv4

・ in-addr.arpa domain

```
4.3.2.1.in-addr.arpa      IN   PTR   www.hogehoge.jp
```

IPv6

・ip6.arpa domain

・Use of ip6.int is recommended since it is backward compatible.

```
0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6
                .arpa          IN   PTR   www.hogehoge.jp
```

[IPv6 address registration concept]

A service with an IPv4 address registered in DNS can add IPv6 compatibility using one of the following two methods.

(1) Register the domain name used for A record also for AAAA record.

(2) Register a domain name for AAAA record that differs from the domain name for A record.

In a migration from IPv4 to IPv6, (1) is normally selected when the user does not need to distinguish between domain names for IPv4 and IPv6. (2) is selected when IPv4 services are to be retained.

DNS records are to be set as described above.

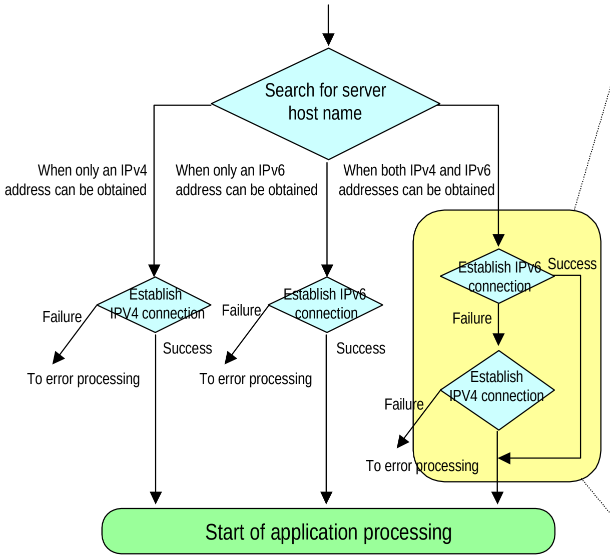
A service with an IPv4 address registered in DNS can add IPv6 compatibility using one of the following two methods.

1. Register the domain name used for A record also for AAAA record.
2. Register a domain name for AAAA record that differs from the domain name for A record.

In a migration from IPv4 to IPv6, (1) is normally selected when the user does not need to distinguish between domain names for IPv4 and IPv6. (2) is selected when IPv4 services are to be retained.

DNS Server Settings (2/2)

Operation flow in making connections to an IPv4/IPv6 compatible TCP application server (Web, mail clients, etc.)


Search for server host name
When only an IPv4 address can be obtained
When only an IPv6 address can be obtained
When both IPv4 and IPv6 addresses can be obtained
Establish IPV4 connection
Failure
To error processing
Success
Establish IPv6 connection
Failure
To error processing
Success
Establish IPv6 connection
Success
Failure
Establish IPV4 connection
Failure
To error processing
Start of application processing

[Precondition]
Most IPv4/IPv6 applications attempt an IPv6 connection before falling back to IPv4.

[Issue]
When an IPv6 connection cannot be established, the time-out occurring when a TCP session is established causes a delay.
Since diagnosing the situation as a failure takes time, start of processing the application in an IPv4 connection is delayed.

[Measures]
・Register only applications for IPv6 that have been verified in DNS.
・Create a mechanism that returns “Unable to connect” in the event of an error.

The following care should be taken in making DNS settings when IPv6 is deployed.

A connection to a TCP application server (Web clients, mail clients, etc.) that supports both IPv4 and IPv6 is performed according to the sequence described in the figure. Most applications that support both IPv4 and IPv6 processes start an IPv6 process before falling back to an IPv4 process.

The problem with this process is that when an IPv6 connection cannot be established, a timeout occurs when the TCP session is established. Since it takes time to detect the failure, there is a delay before application processing starts in the IPv4 connection.

This problem can solved by registering only applications whose operation has been verified by DNS and by implementing a mechanism that returns “Unable to connect” in the event of an error.

5.7.3 MTU Discovery

In IPv4, packets may fragment during transmission and there is no ICMP like ICMPv6 Type 2 for IPv6. Some ISPs use filter ICMP packets for this reason.

However, IPv6 does not fragment packets during transmission. When a router in the transmission path indicates that a packet is too big, it returns a “Packet Too Big Message” (ICMPv6 Type 2) to the sender. When the sender receives this message, it resends packets of appropriate size. Thus communications may deteriorate if an ICMPv6 message (at least Type 2) does not reach the end node in the IPv6 Internet.

It is essential that all parties, including ISPs, not filter ICMPv6 Type 2 messages.

6. IPv6 Deployment Guideline (ISP segment)

6.1 Introduction

This document is intended for operators and system integrators engaged in construction and operation of small-to-medium ISP systems and is a guide to general topics, guidelines and methodology to be discussed by small-to-medium ISPs upon IPv6 deployment.

The information in this document is intended not as a solution but to offer examples that readers can refer to for advice on specific management policies and constraints on the implementation of IPv6.

6.1.1 SWG Members

Chair

Nakai (NTT Communications)

Leaders

Ishihara (KDDI Corporation)	Responsible for address & routing
Ishikawa (NTTPC Communications, Inc.)	Responsible for networking
Matsudaira (Fujitsu Limited)	For networking
Tachibana (aniani.com)	For servers

Members (in alphabetical order)

Arano (Intec NetCore, Inc.)
Inomata (Fujitsu Limited)
Ishihara (Toshiba Corporation)
Kanayama (Intec NetCore, Inc.)
Kawashima (NEC Access Technica, Ltd.)
Kunitake (RINT)
Matsuoka (NTT Information Sharing Platform Laboratories)
Nakahara (NEC Corporation)
Namba (Furukawa Electric Co., Ltd.)
Okamoto (eAccess, Ltd.)
Suzuki (Hitachi, Ltd.)
Suda (Chita Medias Network, Inc.)
Takeyama (eAccess, Ltd.)

6.1.2 Inquiries

For questions related to Part 1, please send email to the following address:

IPv6 Promotion Council of Japan DP-WG

wg-dp-comment@v6pc.jp

6.2 Features of Segment

6.2.1 Affected ISPs

ISPs can be classified into the following categories according to applicable services, service areas and service content.

Applicable services
Wholesale (FLET’S, eAccess, ACCA, etc.), retail (OCN, Nifty, DION, BIGLOBE, etc.)

Geographical scope
Global (UUNET, VERIO, etc.), national (OCN, Nifty, DION, BIGLOBE, etc.), regional (regional ISP)

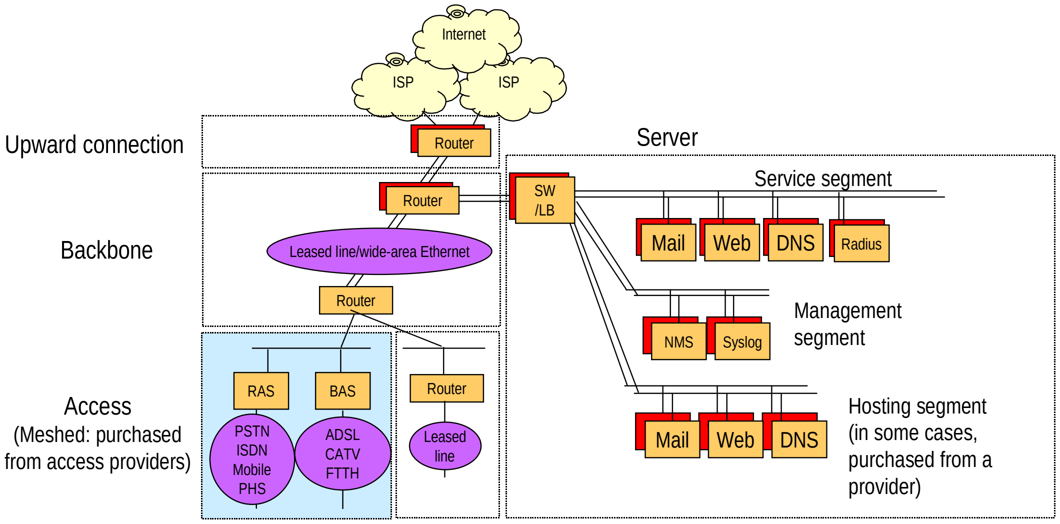
Service content
IP connectivity, applications (ASP), managed service providers (MSP)

This document is intended for general small-to-medium ISPs with the following characteristics.

- The business purchases part of the components from other providers and resells them to general consumers. (retail)
- The business is a second-tier provider rather than a nationwide seller (national - regional)
- The business provides IP connectivity and basic applications (DNS, Web, email)

6.2.2 Components of Small-to-Medium ISPs

Components of small-to-medium ISPs

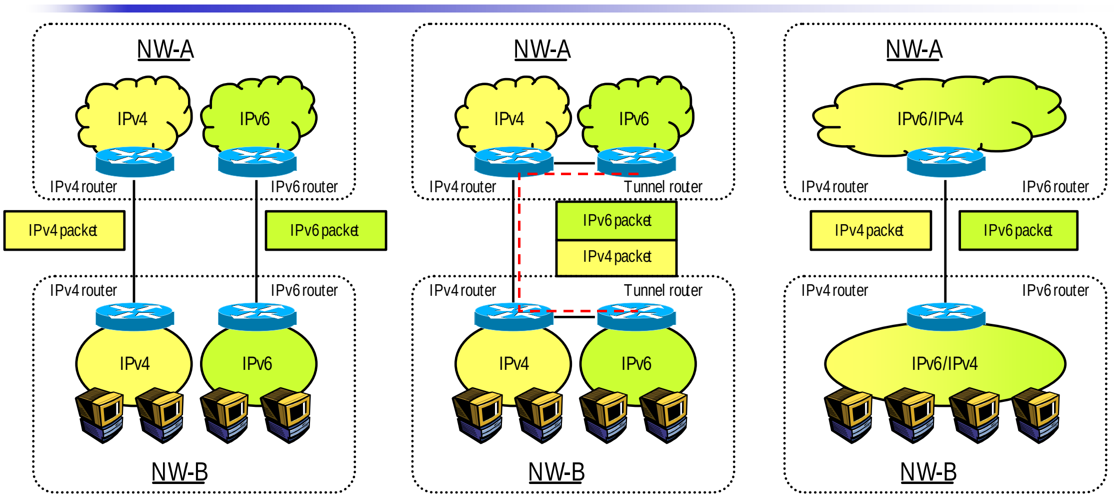


Above is a typical small-to-medium ISP network configuration. Access services such as dialup, ADSL or FTTH are purchased from access providers and, together with the direct leased line connection from the user, are connected to the ISP's own network backbone, which is comprised of a leased line or wide-area Ethernet and which is in turn connected to the Internet via a higher ISP.

The server segment is connected to the backbone. The server segment is comprised of the DNS for the entire service, a service segment that includes email and web servers, a management segment that includes the network management system or syslog server, and a hosting segment that includes web servers that host user web services, email servers and DNS control.

6.2.3 Three Methods for Providing IPv6 Support

Three methods for providing IPv6 support



Native

- Can introduce IPv6 with no impact on the IPv4 environment.
- Most costly.
- Appropriate for cases in which IPv4 stability is critical.

Tunnel

- Can introduce IPv6 with little or no impact on the IPv4 environment.
- Moderate cost.
- Appropriate for cases in which there should be no major impact on the existing IPv4 environment while at the same time making IPv6 available.

Dual

- An ideal method for creating a mixed IPv6/IPv4 protocol environment.
- Minimum cost.
- Appropriate for cases in which all L3 nodes such as routers/firewalls provide dual IPv6/IPv4 support.

There are three methods ISPs can use to provide IPv6 support: native, tunnel and dual. IPv6 support by ISPs means IPv6 communication is implemented for the higher-order connection, the ISP backbone and the user connection, using any of the above three connection modes (or any combination thereof).

Native mode makes it possible to introduce IPv6 with no impact on the IPv4 environment, with the disadvantage being that the migration cost is the highest of the three options. This option is said to be desirable in cases where the stability of the IPv4 environment is critical.

Tunnel mode makes it possible to introduce IP6v with little or no impact on the IPv4 environment. The cost is moderate and this method is desirable in cases in which the existing IPv4 environment is in use and a major impact on the IPv4 environment is deemed unacceptable.

Dual mode provides an ideal option for using a mixed protocol environment (IPv6/IPv4) and the cost is the lowest of the three options. However, all L3 nodes within the ISP including routers and firewalls must provide dual IPv6/IPv4 support.

6.2.4 What is IPv6 Migration for Small-to-Medium ISPs?

What does IPv6 migration mean for small-to-medium ISPs? And what is the motive for ISPs to deploy IPv6?

Possible motivations include:

- Early support for leading-edge services
- Support user needs
- Support national policies and ISP industry trends

Supposing these motivations are true, it would be natural for IPv6 service to be introduced as an additional service rather than as a replacement for existing IPv4 services. In other words, if new IPv6 services are attractive, naturally users will want to use the new services. This means that it is reasonable to expect a phenomenon similar to what happened when users shifted from dialup service to 24-hour ADSL connections, or from fixed-line telephones to ordinary phones plus IP telephone service.

For small-to-medium ISPs expected to launch IPv6 service as a new offering, the following issues must be addressed. The first issue is IPv6 service-related costs. Typical costs include operation, equipment upgrades and user support. Any adverse impact on existing IPv4 service users may produce additional costs. There is no doubt that IPv6-related markets will evolve into sizable scale in near future, however, under the present circumstances it is very difficult to predict when service providers will be able to recoup their investment in stand-alone IPv6 services. It is therefore desirable for small-to-medium ISPs to initially launch IPv6 services on a small scale.

The second issue is the overhead cost incurred by resources such as human resources and know-how required to provide new services. Specifically, in many cases where small-to-medium ISPs operate their business with a minimum of employees, these ISPs may be forced to consider using experimental services to develop of human resources and buildup the know-how necessary for full-blown operation, and as the case may be could be forced to use outsourcing services from other providers.

6.3 Best Current Practices (BCP)

6.3.1 BCP Scope and Reviewing Guideline

The following deals with how to provide experimental or commercial IPv6 services which small-to-medium ISPs can promptly implement on their own. ("BCP" indicates the scope of abilities implemented by small-to-medium ISPs using currently available technology, products and services, excluding methodologies that cannot be achieved by small-to-medium ISPs on their own using non-standard technologies or unavailable products.)

Connectivity, DNS, Web hosting and email are assumed to be the IPv6 services that will be provided, and the disadvantages and advantages of each of the conceivable options are discussed in consideration of the impact on IPv6 services and the rationality of the costs incurred.

6.3.2 Current IPv6 Connectivity Services (Commercial, Experimental)

The following IPv6-based connection services are currently provided.

ISP services

- Leased lines (ATM, STM) Native, dual, tunnel

LAN (DC)	Tunnel, native
ADSL	Tunnel, dual
FTTH	Tunnel
CATV	Dual (experimental), native (experimental)
WLAN	Dual (experimental)
Dialup	Dual (experimental)

IX

- DIX-IE (experimental), JPIX (experimental), JPNAP6 (experimental)

The following issues must be addressed when small-to-medium ISPs provide IPv6 support.

Addressing

- Acquire addresses
- Allocation/assignment

Routing

- EGP
- IGP

Network connections

- Upward connection
- Backbone
- Access

Servers

- Service servers
- Infrastructure servers
- Operation management servers

6.3.3 Addressing

Initial allocation size of addresses

Usage

At the ISP, similar to IPv4 use, IPv6 addressing is used for the following two purposes.

- Address space delivered to the customer (for users)
- Address space for the ISP's own network operation management (for infrastructure)

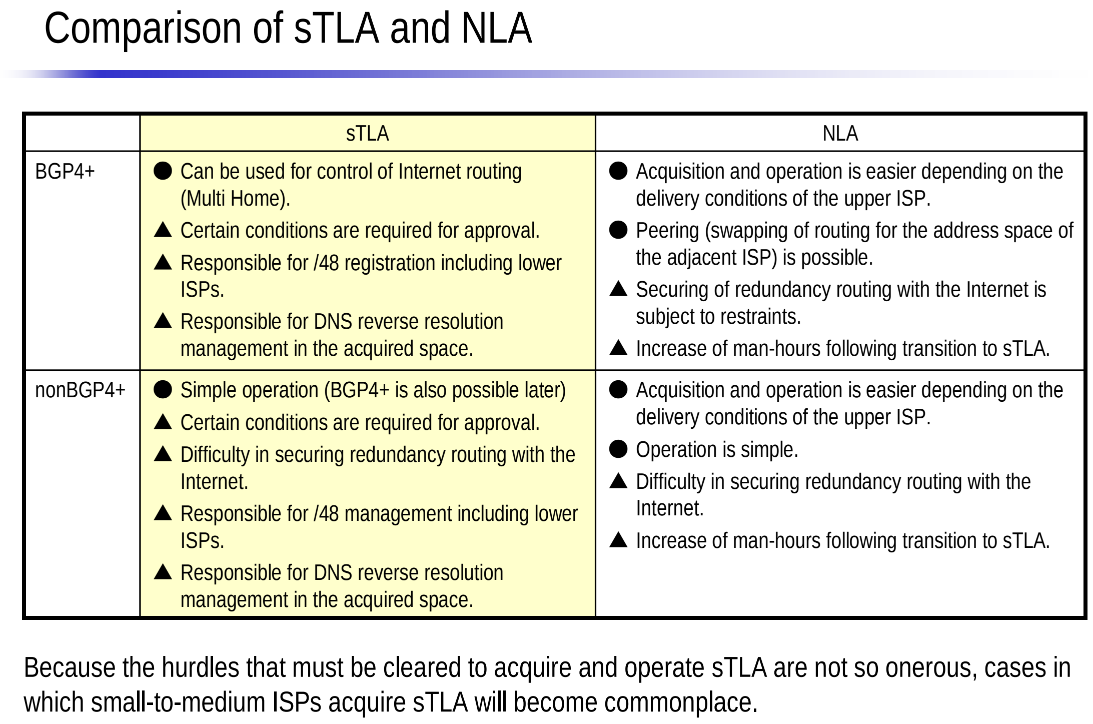
Acquired address space

It can be expected that ISPs may acquire the following two types of IPv6 addresses. As mentioned below, which of the options an ISP selects is determined after considering the size of the in-house network, connection requirements and ease of operation management.

	Size	Method for acquisition
sTLA	Minimum allocation/32 (/35)	Allocated by APNIC (created by JPNIC after submitting an application)
NLA	/33~ /47	Allocated by the owner of sTLA, NLA

Note: The terms sTLA and NLA are not currently in use but because there are no alternative terms they are tentatively used for convenience.

(2) Comparison of sTLA and NLA



Comparison of sTLA and NLA

	sTLA	NLA
BGP4+	● Can be used for control of Internet routing (Multi Home). ▲ Certain conditions are required for approval. ▲ Responsible for /48 registration including lower ISPs. ▲ Responsible for DNS reverse resolution management in the acquired space.	● Acquisition and operation is easier depending on the delivery conditions of the upper ISP. ● Peering (swapping of routing for the address space of the adjacent ISP) is possible. ▲ Securing of redundancy routing with the Internet is subject to restraints. ▲ Increase of man-hours following transition to sTLA.
nonBGP4+	● Simple operation (BGP4+ is also possible later) ▲ Certain conditions are required for approval. ▲ Difficulty in securing redundancy routing with the Internet. ▲ Responsible for /48 management including lower ISPs. ▲ Responsible for DNS reverse resolution management in the acquired space.	● Acquisition and operation is easier depending on the delivery conditions of the upper ISP. ● Operation is simple. ▲ Difficulty in securing redundancy routing with the Internet. ▲ Increase of man-hours following transition to sTLA.

Because the hurdles that must be cleared to acquire and operate sTLA are not so onerous, cases in which small-to-medium ISPs acquire sTLA will become commonplace.

The differences between sTLA and NLA are described above.

When compared with NLA, sTLA has a major advantage over NLA in the degree of freedom ISPs have over routing control. In addition, because the hurdles that must be cleared to acquire and operate sTLA are not so onerous, it is expected that cases in which small-to-medium ISPs supposedly acquire sTLA will become commonplace.

Conditions for address acquisition

Acquisition of sTLA addresses

Conditions for acquisition of sTLA address is set forth in the RIR address policy. The current policy is almost common throughout the entire RIR system, with the following conditions:

- The provider must be an APNIC member or a specified provider of JPNIC address management.
- The provider must support the APNIC address policy.

To qualify for an initial allocation of IPv6 address space, an organization must:

a) be an LIR;
b) not be an end site;
c) plan to provide IPv6 connectivity to organizations to which it will assign /48s, by advertising that connectivity through its single aggregated address allocation; and
d) have a plan for making at least 200 /48 assignments to other organizations within two years.

NLA address acquisition

As described below, because NLA addressing basically depends on the discretion of the upper ISP (having /32) that allocates the addresses, the prerequisite is to satisfy the allocation policy of that ISP.

- In general, the service is combined with use of IPv6 connection service by the upper ISP.
- The allocated address space depends on the policy of the upper ISP, but in many cases, depends on the expected number of /48s after one year (and two years).
- The upper ISP is determined in consideration of the allocated address space and connectivity requirements.

Method for routing control at sTLA

When sTLA is acquired, two options are available to routing control with upper ISPs, using either BGP4+ or static routing. With BGP4+, you can use routing control with IPv6 Internet. In cases where there is only one upper level ISP, static routing alone serves the purpose, but ISPs need to prepare for future BGP4+ operation.

Responsibilities of sTLA owner

Reporting of address assignment to customers

When an sTLA address is acquired, the /48 address space is usually assigned to end users, and that information must be registered that information with APNIC. The report of assignment of /48 to APNIC is sent by mail. Person Object for Tech-c and Admin-c and the inet6num Object are registered.

Reverse resolution of sTLA space DNS

The sTLA owner is expected to be responsible for management of DNS reverse resolution space for the acquired sTLA.

Method to acquire NLA addresses

NLA addresses are acquired from upper ISPs (sTLA , NLA). Address allocation is generally bundled with the use of IPv6 connection service by the upper ISP. The higher ISP for IPv6 connection is not necessarily the same as the upper ISP for IPv4.

While the size of the allocated address space depends on the policy of the upper ISP, in many cases it depends on the expected number of /48s for allocation after one year (and two years). It would be desirable to determine the upper ISP in consideration of the address space to be allocated and the requirements for connection.

Method for routing control at NLA

With NLA, connectivity to an IPv6 interface is acquired from the upper ISP that acquired the NLA address.

From the viewpoint of route integration over the entire Internet in Japan, filters for prefixes longer than /35 are generally used by many ASs. Note that RFC2772 (the 6Bone Backbone Routing Guidelines), which specifies the rules of operation on the 6bone experimental IPv6 network, prohibits punching holes.

Routing also differs depending on the policy of the upper ISP. You can either set the default routing for the upper ISP by a static method, or can receive the full IPv6 route with BGP4+. It is possible to make the route for a specific ISP redundant via Internet Exchange (IX) or private peering. When tacit consensus among ASs is at stake in the future, a major concern will be the impact of the bloated number of routes created by punching holes.

Migration from NLA to sTLA

An ISP that originally started up as an NLA supposedly moves to sTLA when multi-platform is introduced to ensure stability of routing, or when the ISP has a need for larger address space (sTLA) in line with increased consumption of address space for NLA.

The migration entails, for example, acquisition of sTLA first, followed by connection with the higher ISP and IX, then advertisement of sTLA routing, and finally re-numbering processing is conducted. At the same time, the work for address migration arises not only for the ISP’s own site but also at the customer’s site. For details of migration, see Tips & Tricks.

Addressing methods

The following three factors should be considered with respect to configuration of acquired addresses.

- Addressing to customers
- Addressing for network infrastructure
- Addressing for server segment

Addressing to customers

Allocation of addresses for end users is performed in accordance with the IPv6 address policy (http://ftp.apnic.net/apnic/docs/ipv6-address-policy) of the RIR system (APNIC). As a rule, this address policy sets forth allocation of /48s to one connection, but additionally describes alternative options for allocation of /64s in cases in which the customer environment is one segment, or allocation of /128s in case of a single terminal. With the present IPv6 connection service, in general, consumer connections (ADSL, etc.) are allocated a /48 or /64.

Points to keep in mind are:

- Registration of whois with RIR is required in case of /48s,
- Increase of frequency of additional allocation to end users in case of /64s,
- Difficulty in route integration depending on the address backup spare to be reserved.

Addressing in network infrastructure

Compared with IPv4, IPv6 has a large address space, allowing for easier and redundant planning. First of all, all subnets are usually configured with /64s without concern for the number of hosts. In addition, ISPs can allocate /48s for each POP used for infrastructure. Moreover, the ISP is able to favor integration of ISP internal routing over overall address usability.

In case of sTLA (/32), allocation of 7132 incidences of /48 (usability: 10.9%) allows for additional allocation (based on the HD-Ratio (when usability is 0.8)).

ISPs must register with the APNIC database in units of /48, and if the number of entries exceeds HD-Ratio:0.8, immediately upon submitting an application for registration, additional allocation doubles the address space.

It is also desirable to integrate the routing of the addresses for customers by gathering and assigning those addresses for each connection POP (similar to the idea applied to IPv4). At the outset, when a tunnel for customers was terminated at the center server, there was a need to consider renumbering of addresses when a customer migrates to dual service (shifting to the edge).

Addressing for the server segment

For the address space reserved for the server segment, /64 is assigned to a single LAN segment. In order to cope with use of the address space expected in the future (for example, the source address), it is desirable to reserve multiple /64s for a single LAN segment.

6.3.4 Routing

EGP

BGP4+ is used for EGP. Full mesh, route reflector or confederation and other technologies similar to IPv4 BGP are available.

BGP routing topology

In case of external connection (eBGP), whether to separate the lines for each protocol (adding an IPv6 native link) or to perform peering with different routers for IPv4 and IPv6 is subject to the policy of the destination of connection. The peer topology for the internal connection (iBGP) can be performed independently of the IPv4 policy.

For small-to-medium ISPs, in general, both IPv6 and IPv4 use an autonomous system (AS), except for certain circumstances. If the situation differs, depending on the router, chances are that BGP processing of two AS's cannot be run with the same router.

BGP Peer

The following two points should be kept in mind for BGP Peer.

Acceptance of Network Layer Reachability Information (NLRI)

Because reachability information should not depend on other protocols, we recommend that IPv6 NLRI not be handled with IPv4 Peer. In other words, IPv4 routing should be peered by IPv4 address and IPv6 routing should be peered by IPv6 address.

Peer address

Peer addresses are supposedly global address and link-local address. With eBGP, it should basically be subject to the policy of the destination of connection; however, the address policy determines that non-routable global addresses for IX can be assigned to IX. Depending on the specification of eBGP, stable operation is supposedly difficult at the link-local address, so we recommend Global Address be used where available.

Global address is used for iBGP.

BGP routing policy

For routing filters, a prefix filter should be introduced for setup of each peer, and anything other than s/pTLA should be filtered out. In addition, it is desirable to use both the AS Path filter and the prefix filter. Certain measures should be taken to disable punching holes in /35 by /32-based ISPs while admitting 6to4 prefixes (2002::/16). As a precaution, communication with the defunct site local address should be subject to filtering at the external connection interface.

To check the prefix for validity in IPv6, information on s/pTLA should be confirmed with each RIR or with the 6bone database.

Acceptance of routing from upper ISP

Acceptance of IPv6 full routing can be achieved by the use of IPv6 connection service (commercial or experimental) from an upper ISP or by connection to an experimental and research organization such as WIDE. If for reasons having to do with routing stability it is felt that a constant connection service level should be maintained, one recommended method is commercial IPv6 service.

IGP

While OSPFv3, i/IS-ISv6, RIPng, and Static are options for selection of IGP, similar to the case of IPv4, we recommend dynamic routing of Link State method (for which OSPFv3 has already achieved successful operations at a major ISP) as a core IGP.

There are two advantages to the Link State method, convergence of routing is faster and integrated routing can be used. Meanwhile, small scale routing such as initial introduction (tunnel alone) is likely to use Static and RIPng, thus the routing can be initiated with Static or RIPng, then it can be shifted to OSPFv3 to accommodate increases in the number of HOPs or the number of routers that will be handled in the future.

Selection of IGP

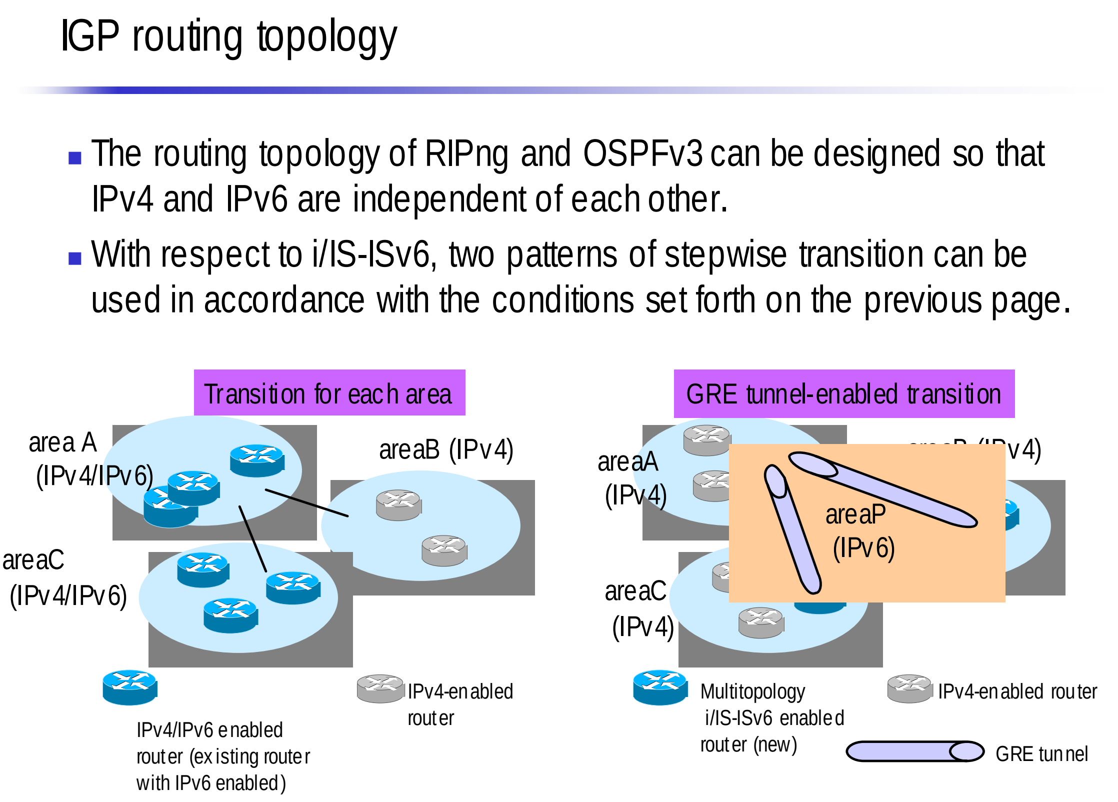
When selecting IGP in IPv6, it is better to select the IPv6 version of the protocol used in IPv4 from the viewpoint of experience with operation. Namely, it would be better to select RIPng when RIP is used in IPv4, or select OSPFv3 when OSPFv2 is in operation.

However, in case of IPv4: i/IS-IS → IPv6: i/IS-ISv6, the following two restraints make it not feasible for stepwise migration.

- Multitopology i/IS-IS is required to make IPv6 routing topology and IPv4 routing topology within the same area independent of each other. (To provide IPv6 support by means of i/IS-IS, all IPv4 i/IS-IS routers operating within the same area should operate in IPv6 as well.)
- Because transport of routing information relies on OSI protocol, it cannot be handled in IPv6 over an IPv4 tunnel. Therefore, introduction of tunnel technology such as GRE tunnel that is independent of the IP protocol is required. The result is increased overhead caused by triple stack configuration of IPv6, GRE, and IPv4.

If such issues matter, IPv4: i/IS-IS → IPv6: OSPFv3 is recommended.

IGP routing topology



IGP routing topology

- The routing topology of RIPng and OSPFv3 can be designed so that IPv4 and IPv6 are independent of each other.
- With respect to i/IS-ISv6, two patterns of stepwise transition can be used in accordance with the conditions set forth on the previous page.

The routing topology for RIPng and OSPFv3 can be designed so that IPv4 and IPv6 are independent of each other. For i/IS-ISv6, according to the conditions set forth in the foregoing section, two patterns of stepwise migration can be used: migration for each area and migration by means of a GRE tunnel.

Routing control with end users

Compared with IPv4, IPv6 requires a certain means of routing control to cope with the increasing chance that end users have a prefix. When dynamic routing is used, filtering is required to prevent an impact on ISP internal components caused by routing advertised from the user.

When using RA on a segment shared by two or more users, if a user issues SA by mistake, you must perform filtering using a switch or modem, or, though it is not the ideal method, set router-preference to high at upper routers.

6.3.5 Network

Upward connection

The menu provided by upper ISPs can be classified into the following categories:

Connection method: Tunnel, native, L2 sharing, dual
Routing protocol: BGP4+, static

The configuration pattern for upward connection is supposed to be dedicated to IPv6 service or to be shared by IPv4 and IPv6 service.

As used here, the term “dedicated” means that no IPv4 user traffic is allowed and does not mean that the router only runs IPv6 service. For the time being, a router dedicated to IPv6 service has to be operated with a dual stack for the sake of router management (SNMP, etc.).

Each menu provided by upper ISPs has the following features:

Tunnel type, L2 sharing type

These methods are often charged as an additional service to IPv4.

Dual type

This method does not require a new line and is less expensive than the purchase of both IPv4 and IPv6 services.

Native type

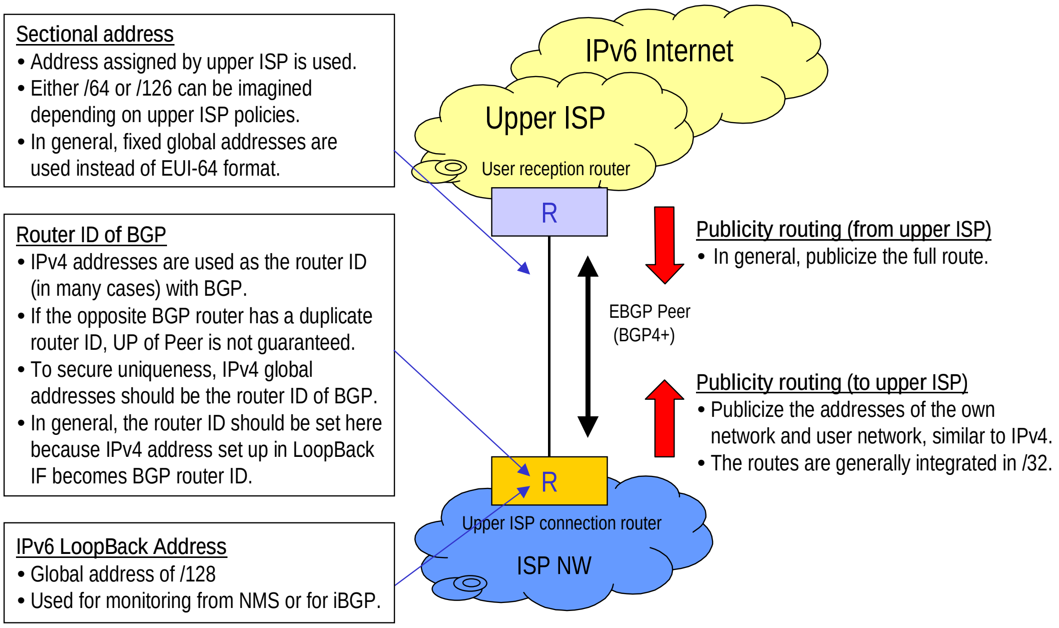
This method may be expensive if it requires a line dedicated to IPv6 due to the geographical distance from the upper ISP.

In addition to the foregoing matters, measures for available routing protocols (BGP4+, Static), charges, and modification to the menu in the future will be discussed and eligible upper ISPs will be chosen.

Concerning the upward connection router on the ISP side, failure in the upward connection router may impact all existing services, so for operational security reasons routers should be allocated separately for both the new service (IPv6) and existing service (IPv4), which requires stable operation. (This can also be handled with types other than dual type). Installation of a dedicated IPv6 router may be disadvantageous in terms of the equipment investment.

A configuration example of upward connection at small-to-medium ISPs is shown below.

Configuration example of upward connection (BGP4+)



Sectional address
- Address assigned by upper ISP is used.
- Either /64 or /126 can be imagined depending on upper ISP policies.
- In general, fixed global addresses are used instead of EUI-64 format.

Router ID of BGP
- IPv4 addresses are used as the router ID (in many cases) with BGP.
- If the opposite BGP router has a duplicate router ID, UP of Peer is not guaranteed.
- To secure uniqueness, IPv4 global addresses should be the router ID of BGP.
- In general, the router ID should be set here because IPv4 address set up in LoopBack IF becomes BGP router ID.

IPv6 LoopBack Address
- Global address of /128
- Used for monitoring from NMS or for iBGP.

Publicity routing (from upper ISP)
- In general, publicize the full route.

Publicity routing (to upper ISP)
- Publicize the addresses of the own network and user network, similar to IPv4.
- The routes are generally integrated in /32.

Backbone

The backbone at small-to-medium ISPs can be defined as the line connecting the installed base of the upward connection router and the access point. As defined here, the term access point refers to the connection point wired to the access carrier. In this case, the access point is not always furnished with a router. In general, small-to-medium ISPs purchase a backbone line from another common carrier. A recent trend is to purchase wide-area Ethernet services. Purchase of the backbone line is occasionally taken as a synonym for construction of a backbone.

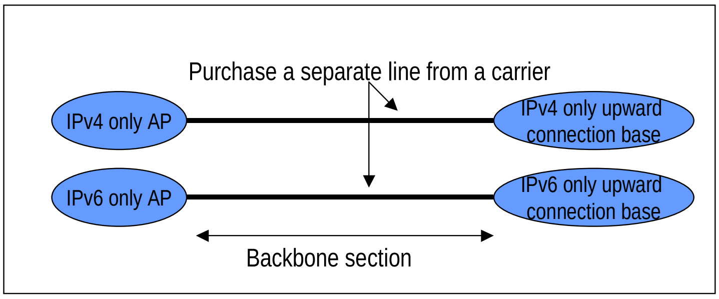
There are four basic backbone configurations: separate line (dedicated to IPv6 service) type, tunnel type, line sharing (L2 separation) type and dual type.

① Separate line (dedicated to IPv6 service) type

Separate line type (line dedicated to IPv6 service)

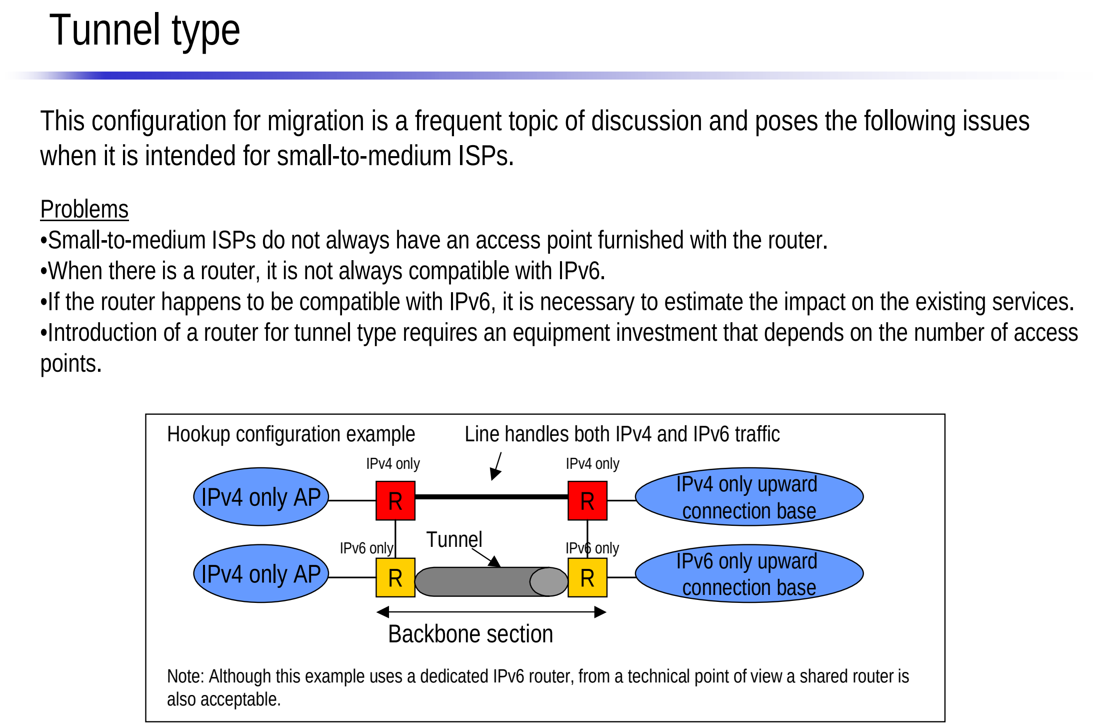
- With this pattern, a separate line is purchased for IPv6.
- An advantage is the lack of impact from traffic caused by other services.
- A disadvantage is increased line costs incurred by other line wiring.

Hookup configuration example


Purchase a separate line from a carrier
IPv4 only AP
IPv4 only upward connection base
IPv6 only AP
IPv6 only upward connection base
Backbone section

This pattern denotes purchase of a separate line for IPv6 and has the advantage of freedom from impact by traffic for the other service. A disadvantage is the expense of line costs incurred by the need for another line connection.

② Tunnel type



Tunnel type

This configuration for migration is a frequent topic of discussion and poses the following issues when it is intended for small-to-medium ISPs.

Problems

•Small-to-medium ISPs do not always have an access point furnished with the router.

•When there is a router, it is not always compatible with IPv6.

•If the router happens to be compatible with IPv6, it is necessary to estimate the impact on the existing services.

•Introduction of a router for tunnel type requires an equipment investment that depends on the number of access points.

Hookup configuration example

Line handles both IPv4 and IPv6 traffic
IPv4 only
IPv4 only
IPv4 only AP
R
R
IPv4 only upward connection base
IPv6 only
Tunnel
IPv6 only
IPv4 only AP
R
R
IPv6 only upward connection base
Backbone section

Note: Although this example uses a dedicated IPv6 router, from a technical point of view a shared router is also acceptable.

This configuration for migration is a frequent topic of discussion and poses the following issues when it is intended for small-to-medium ISPs.

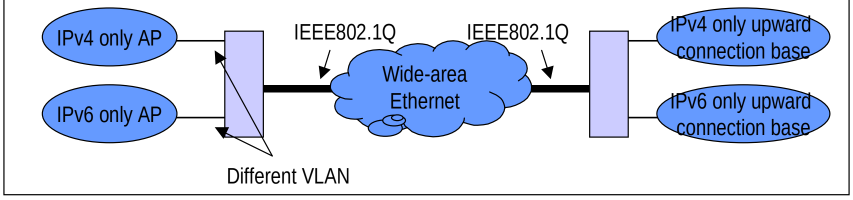
- Small-to-medium ISPs do not always have an access point furnished with the router.
- When there is a router, it is not always compatible with IPv6.
- If the router happens to be compatible with IPv6, it is necessary to estimate the impact on the existing services.
- Introduction of a router for tunnel type requires an equipment investment that depends on the number of access points.

③ Line sharing (L2 separation) type

Line sharing (L2 separation) type

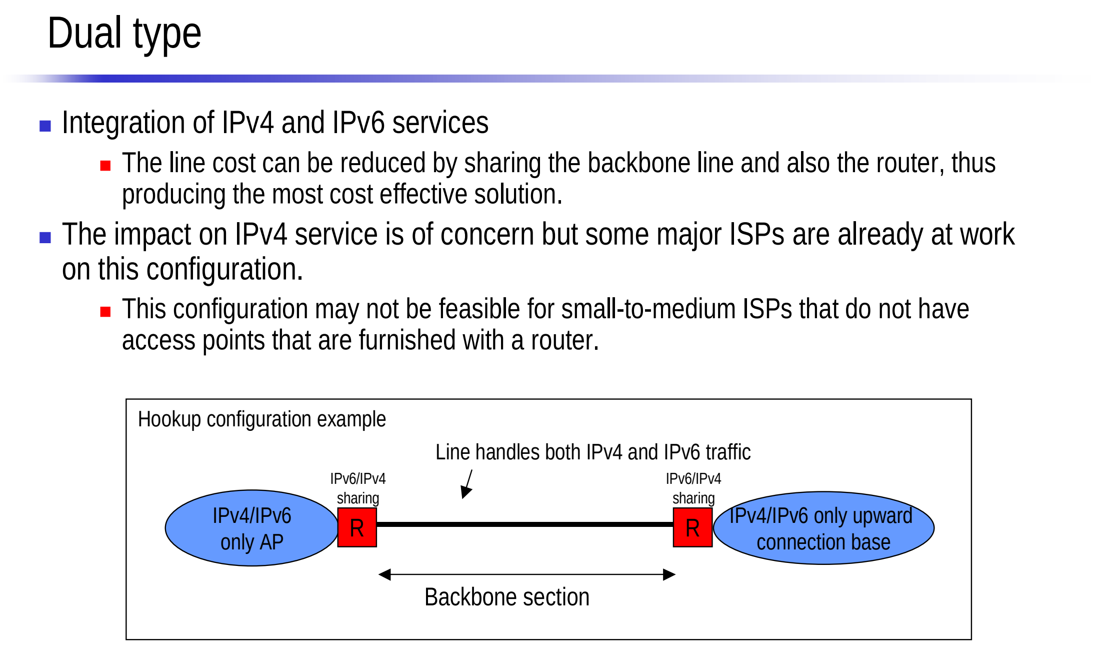
- The existing IPv4 service and IPv6 service are logically separated from each other via L2 technology.
    - VLAN is used on Ethernet and VP/VC is used on ATM.
- Line costs can be reduced by sharing IPv4 and IPv6 services on the backbone line.

Hookup configuration example



This configuration is intended to logically separate the existing IPv4 service and IPv6 service by means of layer 2 technology, whereas VLAN is used on Ethernet and VP/VC and other mechanisms are used on ATM. This method reduces the line cost by sharing IPv4 and IPv6 services on a backbone line.

④ Dual type



Dual type

- Integration of IPv4 and IPv6 services
  - The line cost can be reduced by sharing the backbone line and also the router, thus producing the most cost effective solution.
- The impact on IPv4 service is of concern but some major ISPs are already at work on this configuration.
  - This configuration may not be feasible for small-to-medium ISPs that do not have access points that are furnished with a router.

Hookup configuration example
Line handles both IPv4 and IPv6 traffic
IPv6/IPv4 sharing
IPv4/IPv6 only AP
R
IPv6/IPv4 sharing
R
IPv4/IPv6 only upward connection base
Backbone section

This configuration is intended to provide IPv4 service and IPv6 service on an integrated basis. It is the most economical connection type and reduces cost by sharing the backbone line and also the router. While the threat to IPv4 services is of concern, some major ISPs are already at work on this configuration. Conversely, some small-to-medium ISPs are faced with difficulty in this configuration because access points may not be furnished with a router.

The following illustration is an example of configurations that are expected to be used at many small-to-medium ISPs.

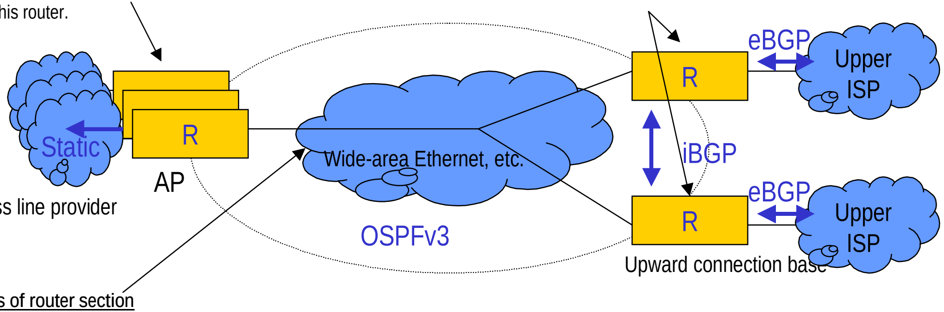
Backbone configuration example

Router for each AP

- Sets the routing for integrated customers by static routes.
- Redelivers the static route to OSPFv3.
- The access line provider may occasionally deliver the function of this router.

Router at upward connection base

- Originates the default route for OSPFv3.
- It is unnecessary to redeliver the routing from the upper ISP, which is learning in BGP, to OSPFv3.



Address of router section

- Assigns the sectional address with /64.
- /126 is acceptable in cases of connection by Point to Point for POS, but it is preferably designed with /64 to deal with the chance that the configuration will be changed later.
- Uses the fixed global address instead of EUI-64 format.
- When using EUI-64 format, change of registration for NMS may arise each time the router is replaced.

Router ID of OSPFv3

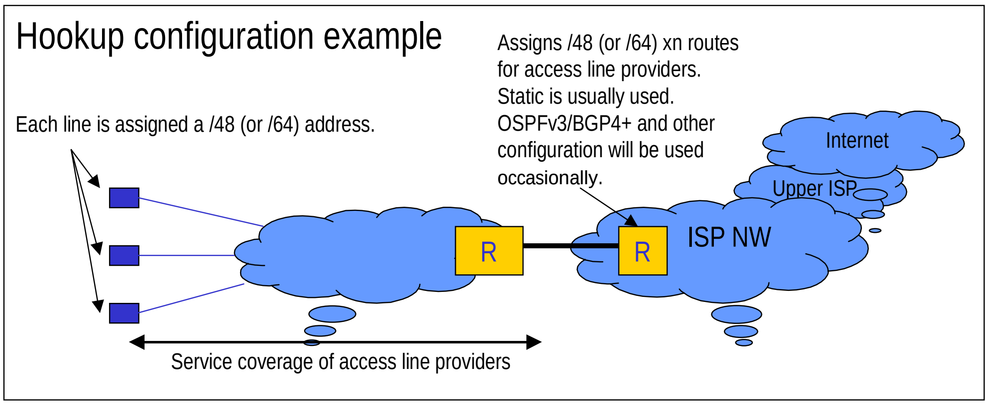
- 32bit router ID is used in OSPF.
- The router ID in the same OSPF must be unique.
- Many routers use the IPv4 address set in LoopBack IF as the router ID.
- It is preferred to use IPv4 global addresses to secure uniqueness.

Access

It is assumed that ADSL and FTTH or dialup will be used for the access line carrying IPv6 service provided by small-to-medium ISPs. It has become a general trend for small-to-medium ISPs to purchase those communication services from access carriers and deliver IPv6 services. This document discusses this type of configuration.

Connection with access line provider

- Among access lines (PPP, etc.), models terminated in the network of the access line provider are expected to be the mainstream.
- It is assumed that models that terminate PPP on the ISP side will be rare.



Hookup configuration example

Assigns /48 (or /64) xn routes for access line providers. Static is usually used. OSPFv3/BGP4+ and other configuration will be used occasionally.

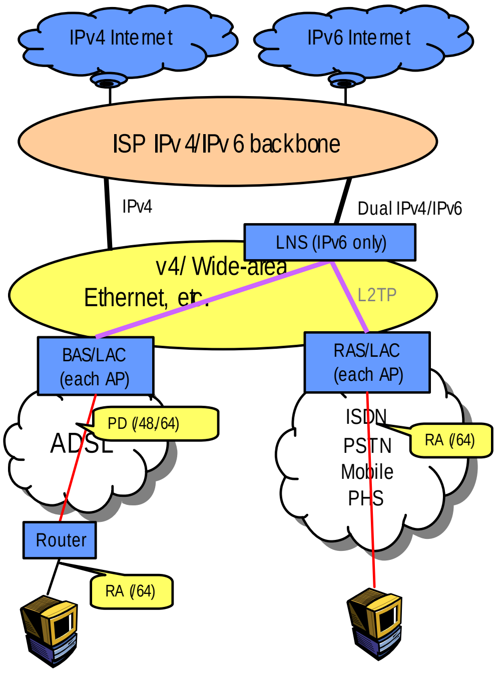
Each line is assigned a /48 (or /64) address.

Service coverage of access line providers

From this point on models that terminate within the network of access carriers are expected to become the mainstream for each access line (such as PPP). It is assumed that models that terminate PPP on the ISP side will be rare.

Dual delivery configuration of ADSL and dialup (1)

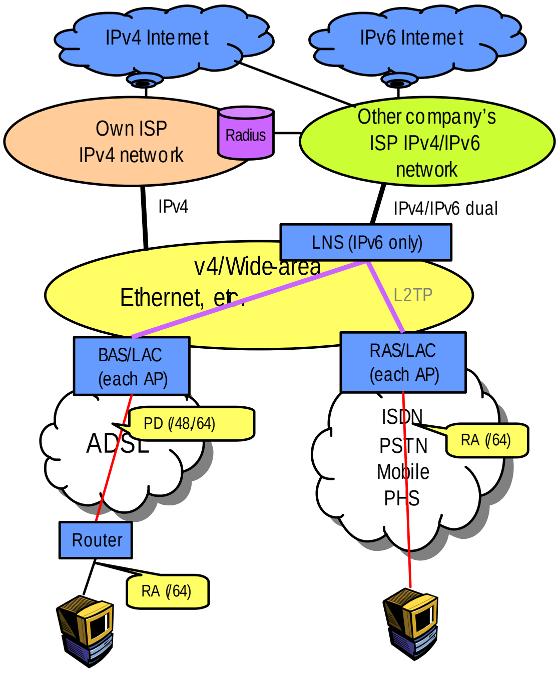
- Currently, services are generally collected from BAS/RAS at each access point of the access line provider and sent to an IPv6-compliant LNS by means of L2TP.
    - It is unnecessary to make the BAS and RAS at the access points IPv6-compliant.
- As before, small-to-medium ISPs are able to deliver dual ADSL and dialup service of by enabling dual connection with the access line provider.



The current measures to ensure compliance with IPv6 are typically represented by integration of services in an IPv6-compliant LNS using L2TP from BAS/RAS at each access point of the access line carrier. This is because BAS/RAS at each access point need not be compliant with IPv6. As usual, small-to-medium ISPs will be able to provide dual services through ADSL and dialup by means of dual connection with the access line carrier.

Dual delivery configuration of ADSL and dialup (2)

- Another configuration for small scale implementation is to outsource all IPv6 external connection/backbone services to another provider.
  - IPv6 addresses are registered for each customer account in the in-house Radius.



Another method for initiating small scale start of operations includes outsourcing of the entire IPv6 external connection/backbone to other providers. In this case, IPv6 addresses are registered for each customer account in the in-house Radius.

Delivery type by tunnel

IPv6 over IPv4 tunnel

Overall service charges will grow as IPv4-fixed global addresses are increasingly required. On the other hand, dual services have already been delivered by many ISPs, whereas, they can be delivered with each at relatively low prices by simply preparing one tunnel server unit.

DTCP (Dynamic Tunnel Configuration Protocol)

DTCP is furnished with an authentication function and can be used with IPv4 dynamic addresses. (Coordination with existing accounts is made possible by means of Radius.) Some ISPs independent of IPv4 ISPs are delivering services. It is possible to deliver the service with each at relatively reasonable prices by simply preparing one tunnel server unit.

6.3.6 Server

Classification of servers

Servers running at ISPs can be classified into the following categories.

Service server

This is an application server practically used by users that has Web and email functions. Depending on the need, it is customized in various ways to implement ISP publicity web services, hosting and web and email bundled with connection services.

Infrastructure server

This server is mostly commonly required when using services and it refers to the DNS or Radius. It is claimed to be the most reliable portion of the system.

Operation server

Required for an ISP to operate, this type of server is represented by NMS and SNMP. It is not a target of direct access by users and IPv6 support is not mandatory.

Server support for IPv6

Concerning the present state of server support for IPv6, many OSs used on servers are capable of dual stack configuration (Linux, FreeBSD, Solaris, etc.). Most existing IPv4 applications (web access, email, DNS, etc.) already support IPv6. DNS and web are already on the list of achievements in commercial and experimental services at ISPs.

Methods of providing IPv6 support

Two methods can be used to configure IPv6 support: use of either dual IPv4 service servers or additional servers dedicated to IPv6 service. If the dual option does not eliminate the possibility of an impact on IPv4 performance, the latter method is a valid alternative. The latter method should be used if introducing a dual configuration will make it likely there will be a loss of service upon upgrading the OS or applications.

The server is installed in a new dual segment dedicated to IPv6 service. The reason for this is that there could be an impact on the IPv4 server when IPv6 and IPv4 servers with different response speeds for dealing with fragility in the system are installed in the same segment; however, the server is not nearly as large a cost factor as the backbone itself.

Care should be taken with regard to filtering of ICMPv6 in the IPv6 server segment. Fragmentation processing in IPv6 is not performed at the intermediate node and messages are divided into deliverable sizes by the sender terminal by means of Path MTU Discovery (using ICMPv6 type2 messages), thus ICMPv6 type2 messages should not be filtered at the intermediate router.

DNS

There are two aspects to DNS IPv6 support: the ability to perform IPv6 address resolution and execution via IPv6. Name resolution in IPv6 includes, of course, two options: forward resolution from the host name to IPv6 address (AAAA record) and reverse resolution from the IPv6 address to the host name (ip6.arpa. domain).

We recommend the BIND9 for DNS implementation be used. BIND9 supports IPv6 at all points and has a successful record of achievement through commercial delivery. This is also true with respect to BIND8. For name resolution only (via IPv4), BIND4 is also OK.

Concerning the method for IPv6 support at the ISP, because the DNS is the most important server and no service outage is acceptable, two additional dedicated IPv6 dual servers (primary and secondary) are prepared. The resolver and zone management may be shared.

This method provides a dedicated IPv6 resolver. The existing server can be used for inquiry via IPv4. Upon request, reverse delegation or a customer-managed secondary DNS server can also be provided.

Web

Web servers are classified into ISP publicity web services, web services bundled with connection services and web hosting.

Software support has already been demonstrated for Apache 2.0 and later and there is a record of successful performance at ISPs.

Concerning the method of compliance, first of all, the ISP publicity web should be considered. It is not such a critical matter compared with the DNS, but if safety is of paramount importance, a new dual server stack should be installed. To cope with Apache 2.0 and later, an alternative is to turn an existing server into a dual stack server.

Dual implementation of web bundled with ISP service and web hosting is likely to be postponed, the reason being that many small-to-medium ISPs use services delivered by hosting providers whose dual implementation is in a premature stage.

Introduction of a new dual server is considered to be an autonomous solution; however, the problem with this is that if there are a large number of servers large service charges may be assessed for transferring contents, and moreover, mirroring of contents and a synchronization mechanism are also required, thus increasing operation man-hours.

On the other hand, introduction of a reverse proxy under dual stack is a realistic solution. As a result, it becomes easier to provide access to an existing IPv4 server from IPv6 while avoiding the need to transfer content, thus producing a good solution when there is only limited IPv6 access.

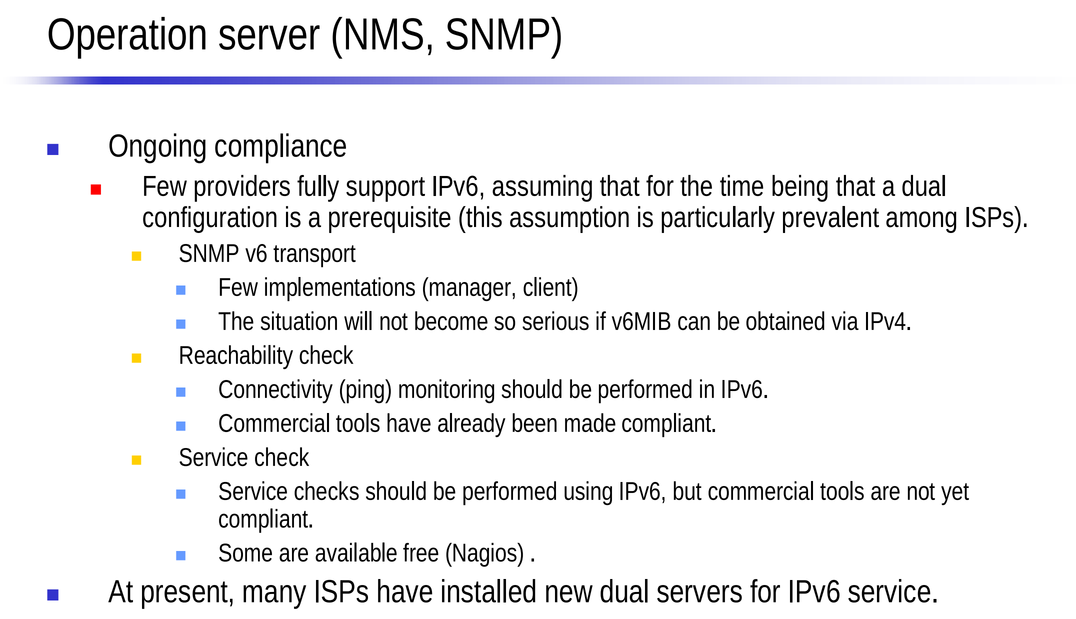
Mail

About mail server software, Sendmail 8.1 and later provides IPv6 support. Qpopper includes a patch that provides IPv6 support, however, compared to DNS and Web use, this product is not as commonly used.

Under the present circumstances, BCP antivirus software does not support IPv6, so it is recommended that provisioning by ISP services be avoided. In short, the measures to be taken at present should be such that SMTP and POP servers should not support IPv6, and no IPv6 address should be assigned to the host name in the DNS MX record.

When the above mentioned problems are solved, it is assumed that two options will provide IPv6 support. First, with regard to existing mail accounts, a new dual server is installed and the disk of the existing IPv4 server is shared by NFS and other systems. Second, if new mail accounts are going to be set up a new dual server is installed.

Operation server (NMS, SNMP)



Operation server (NMS, SNMP)

- Ongoing compliance
  - Few providers fully support IPv6, assuming that for the time being that a dual configuration is a prerequisite (this assumption is particularly prevalent among ISPs).
    - SNMP v6 transport
      - Few implementations (manager, client)
      - The situation will not become so serious if v6MIB can be obtained via IPv4.
    - Reachability check
      - Connectivity (ping) monitoring should be performed in IPv6.
      - Commercial tools have already been made compliant.
    - Service check
      - Service checks should be performed using IPv6, but commercial tools are not yet compliant.
      - Some are available free (Nagios) .
- At present, many ISPs have installed new dual servers for IPv6 service.

Because the dual stack network is deemed a prerequisite for the time being (specifically for ISP) for IPv6 support by operation servers (NMS, SNMP), very few products fully support IPv6. In particular, there have been very few implementation of IPv6 transport of SNMP on both a manager and client basis. At the same time, the situation will not get much worse if IPv6 MIB is made available via IPv4.

With respect to reachability check, monitoring of connectivity (ping) should be performed under IPv6, and commercial tools support such requirements.

Service checks should be performed under IPv6, but commercial tool do not yet provide such support. Some tools are available free of charge (Nagios).

At present, many ISPs have installed new dual servers dedicated to IPv6 service.

6.4 Assumed Configuration and Issues for the 50-50 ratio

6.4.1 Assumed Configuration and Issues for the 50-50 Ratio

When the ratio of IPv4 to IPv6 reaches 50-50, the following situations and issues may arise.

Increase in ratio of dual system equipment

Stable operation as a dual system should be ensured, and fallback operation from IPv6 to IPv4 by the application should be done with little trouble. Moreover, issues to be worked out include the measures taken to make possible anything currently impossible under IPv6 that can be performed with IPv4, including automatic DNS detection method, compliance of SNMP with IPv6 transport, IPv6 support in antivirus software, StatefulAutoConfiguration (DHCPv6), multi-platform connection of end sites, multi-platform connection using PI addresses and ICMPv6 filtering.

Growth in IPv6 traffic

Improvement in processing performance with respect to routers, SW, IDS, FW, and load dispersing device is called for.

Emergence of IPv6-only devices

When a device responsive only to IPv6 appears, it is necessary to check for the ability to communicate with IPv4 only equipment and the method for communication. As mentioned later, migration of IP telephones to IPv6 is also conceivable. Where a translator is required, the type and installed location should also be considered.

Utilization of Internet by non-PC equipment

It is a MUST to consider tools for arrangement of contents and implementation of Zero-conf, and develop a method for simple security measures.

Access from outside to inside

Standardization of a dynamic punching hole protocol is desirable for remote access to internal components. Also called for should be improvements in mutual connectivity of IPsec and establishment of a security management method (mentioned later) by ISPs. In addition, it is also necessary to determine a protective means for traffic of the control system, which is narrow-band but important when conducting maintenance and measurement from remote systems.

Growth in P2P traffic

In conjunction with the growth in P2P traffic, a traffic control method will be called for (for example, discrimination between file swapping and IP telephones).

Integration of broadcasting and communications

A stepwise plan should be considered to promote default assumption of the multicast function up to home electronics. It is also expected to be necessary to establish a quality differentiation method against Best Effort Service (QoS, policy routing (mentioned later)).

IP communication with mobile equipment

In particular, operation of seamless Mobile IPv6 is called for when the link is changed.

Others

Other issues that need to be worked out include name resolution technologies (such as DNS, UPnP, SIP, etc) and their usage (classification), usage of Privacy Extension, and establishment of consensus among ISPs for the problems arising in the source of operation (such as establishment of the standard for punching holes or recommendation of Ingres filter at the provider edge). In addition, compliance of the ISP with the configuration to be assumed by each segment (Home, Unmanaged, Managed) is called for.

6.4.2 Migration of IP Telephony to IPv6

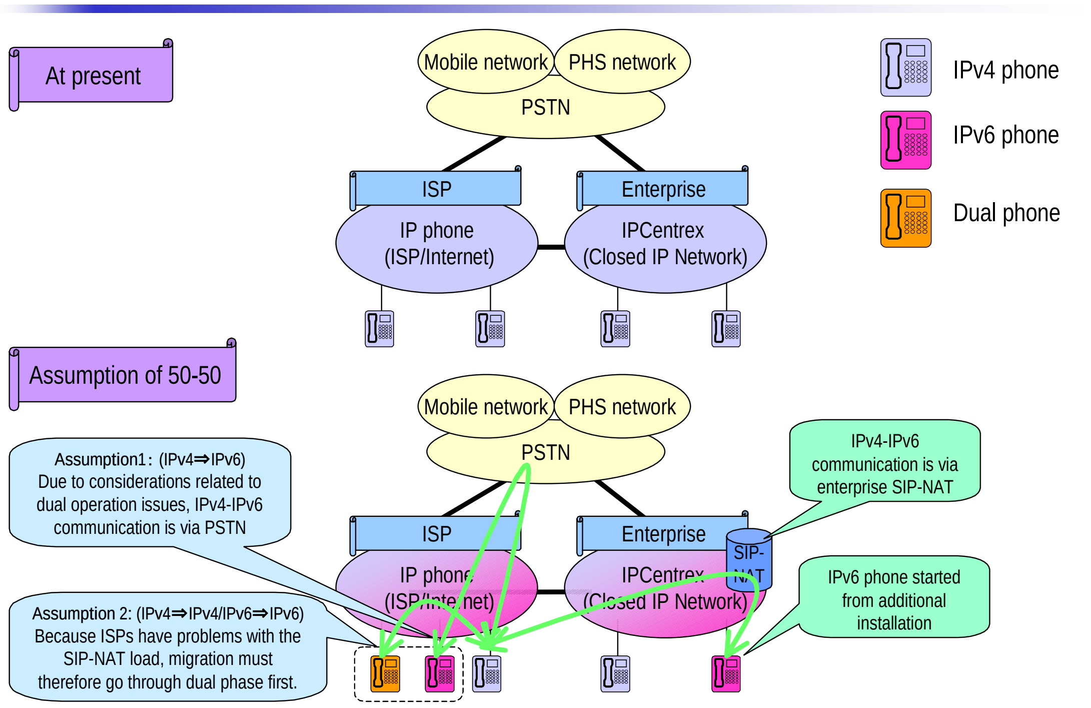
There are two issues to be worked out by ISPs with respect to migration of IP telephones to IPv6: migration of IP telephones provided by ISP and interconnection with corporate IP Centrex.

Specifically, the issue varies depending on whether dual telephones can exist in the course of migration of IP telephones. If a dual telephone matters, the problem is whether to ensure satisfactory reliability of operation including a mechanism of protocol selection between the SIP server and the client as well as fallback (see Assumption 1 in the illustration below).

When only an IPv6 only telephone matters, the problem is how to establish connection with IPv4 equipment, and in particular, whether a translator like SIP-NAT can fully withstand the load is also a problem (see Assumption 2 in the illustration below).

Under the present circumstances, many small-to-medium ISPs are purchasing IP telephone service from major ISPs (outsourcing SIP servers), whereas, it is conceivable that there are few examples of those ISPs being aware of IP telephone migration to IPv6.

Assumptions for transition to 50-50



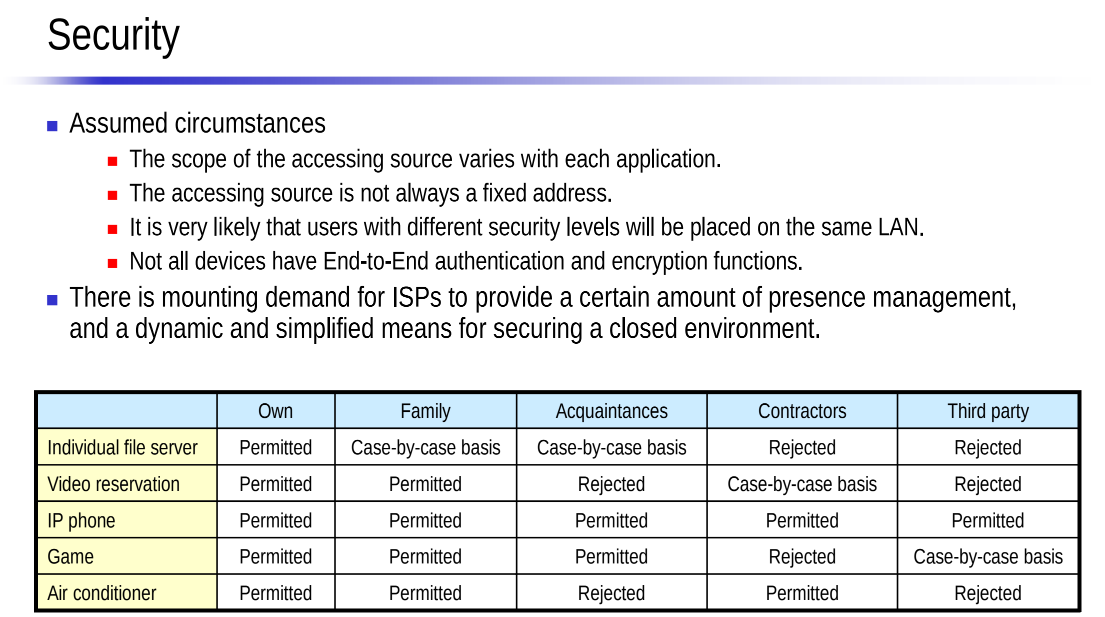
Assumption1: (IPv4⇒IPv6)
Due to considerations related to dual operation issues, IPv4-IPv6 communication is via PSTN

Assumption 2: (IPv4⇒IPv4/IPv6⇒IPv6)
Because ISPs have problems with the SIP-NAT load, migration must therefore go through dual phase first.

IPv4-IPv6 communication is via enterprise SIP-NAT

IPv6 phone started from additional installation

6.4.3 Security



Security

- Assumed circumstances
  - The scope of the accessing source varies with each application.
  - The accessing source is not always a fixed address.
  - It is very likely that users with different security levels will be placed on the same LAN.
  - Not all devices have End-to-End authentication and encryption functions.
- There is mounting demand for ISPs to provide a certain amount of presence management, and a dynamic and simplified means for securing a closed environment.

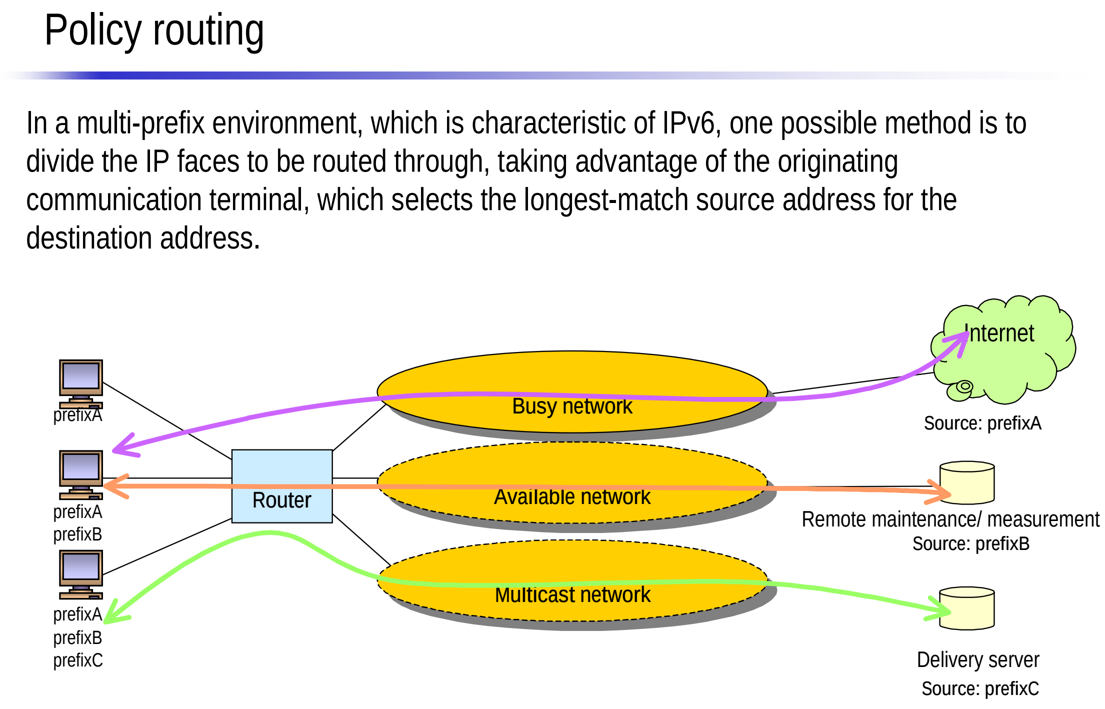
	Own	Family	Acquaintances	Contractors	Third party
Individual file server	Permitted	Case-by-case basis	Case-by-case basis	Rejected	Rejected
Video reservation	Permitted	Permitted	Rejected	Case-by-case basis	Rejected
IP phone	Permitted	Permitted	Permitted	Permitted	Permitted
Game	Permitted	Permitted	Permitted	Rejected	Case-by-case basis
Air conditioner	Permitted	Permitted	Rejected	Permitted	Rejected

With respect to the security about IPv6, the following conditions will supposedly be revealed in comparison with IPv4.

- The scope of the accessing address varies depending on the application.
- The accessing source is not necessarily a fixed address.
- Some users having different security levels are very likely placed on the same LAN.
- Every device does not necessarily have end-to-end authentication and encryption functions.

Under these circumstances, there is mounting demand for ISPs to provide a certain amount of presence management, and a dynamic and simplified means for securing a closed environment.

6.4.4 Policy Routing



Policy routing

In a multi-prefix environment, which is characteristic of IPv6, one possible method is to divide the IP faces to be routed through, taking advantage of the originating communication terminal, which selects the longest-match source address for the destination address.

With IPv6, two or more network prefixes can be assigned to each terminal. As a result, multiple addresses can be assigned. It is then possible to select a source address which is the longest-match for the destination address to communicate with. This mechanism is set forth in RFC3484. It is assumed that this mechanism will the communication channels to be selected separately.

6.5 Tips & Tricks

6.5.1 Address-related Matters

Manual setting is recommended for router and server addresses. The reason for this is that automatic configuration via EUI-64 may cause the address to be changed when the NIC changes.

An alternative is to consider a self-explanatory naming convention in order to relieve the effort on DNS registration and filtering setting, as mentioned below.

- ::Express port numbers or names by freely combining 0~9 and a~f, including :53, ::80 and ::café.
- Express ATM link between Tokyo 03 – Hiroshima 082 using c726:a00:3:82.
  Careful attention should be taken when using such self-explanatory addresses, which are vulnerable to cyber attacks.

6.5.2 Renumbering Convention

The ability to assign multiple IPv6 addresses to the same interface provides the means to perform renumbering through coexistence of both new and old addresses.

Perform the following steps.

Acquire a new address, then, using the new address, configure connectivity (routing) settings.

Assign the new address to the IPv6 node (the router and the terminal).

At the same time, assign the old address instead of deleting it.

Automatic address configuration is used at the terminal level.

In conjunction with the previous step, work such as changing the DNS registration is performed.

Next, the old address is deleted, as is the old address connectivity (routing).

The above procedure provides the means to perform stepwise renumbering with less impact on service than under IPv4.

6.5.3 Method of sTLA Acquisition

Refer to the application Web for initial acquisition of sTLA.

http: //www.apnic.net/services/ipv6_guide.html (APNIC)
http: //www.nic.ad.jp/ja/ipv6/index.html (JPNIC)

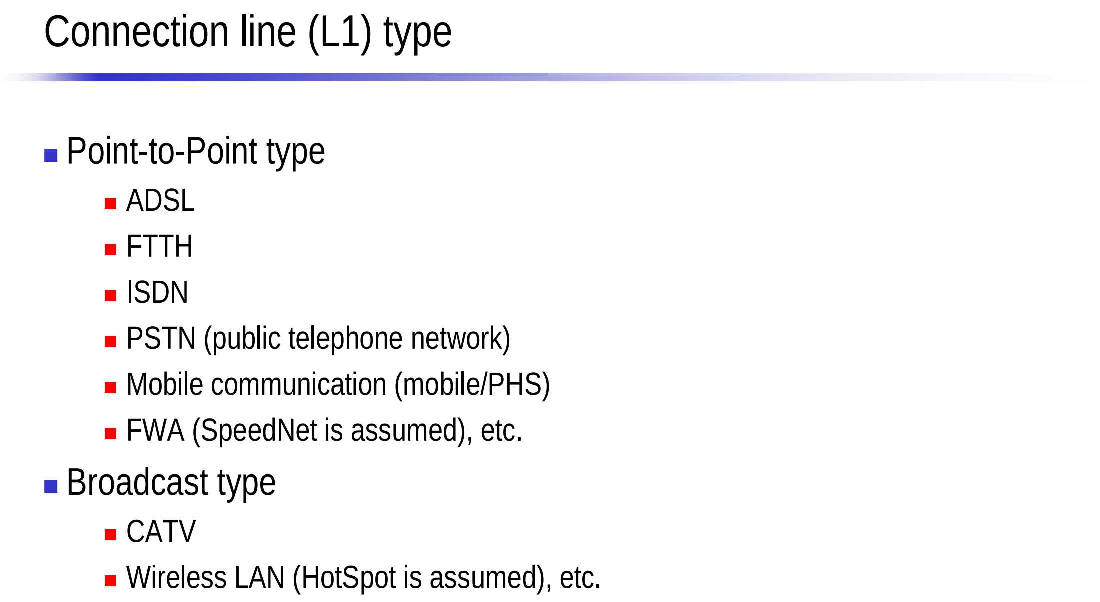
Next, an application is filed with each authority through the Web. APNIC members should file the application with APNIC, and providers authorized for JPNIC address management should file the application with JPNIC. After confirmation of the particulars of the application, as of February 2004, assignment of sTLA will be approved in approximately one month.

Historic process of sTLA assignment

The assignment policy for the first sTLA set forth in 1999 stipulated the initial minimum assignment would be /35, but it was changed to /32 in accordance with an amendment on July 1, 2002. sTLA owners eligible for existing /35s may optionally upgrade to /32 but after the policy went into effect some elected to stay with /35. There are therefore currently sTLA owners of both /32 and /35.

6.6 Appendix (Access)

6.6.1 Communication Line (L1) Type

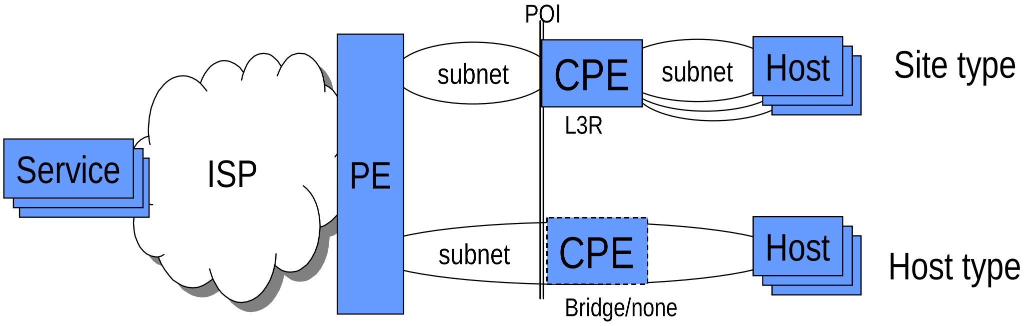


Connection line (L1) type

- Point-to-Point type
  - ADSL
  - FTTH
  - ISDN
  - PSTN (public telephone network)
  - Mobile communication (mobile/PHS)
  - FWA (SpeedNet is assumed), etc.
- Broadcast type
  - CATV
  - Wireless LAN (HotSpot is assumed), etc.

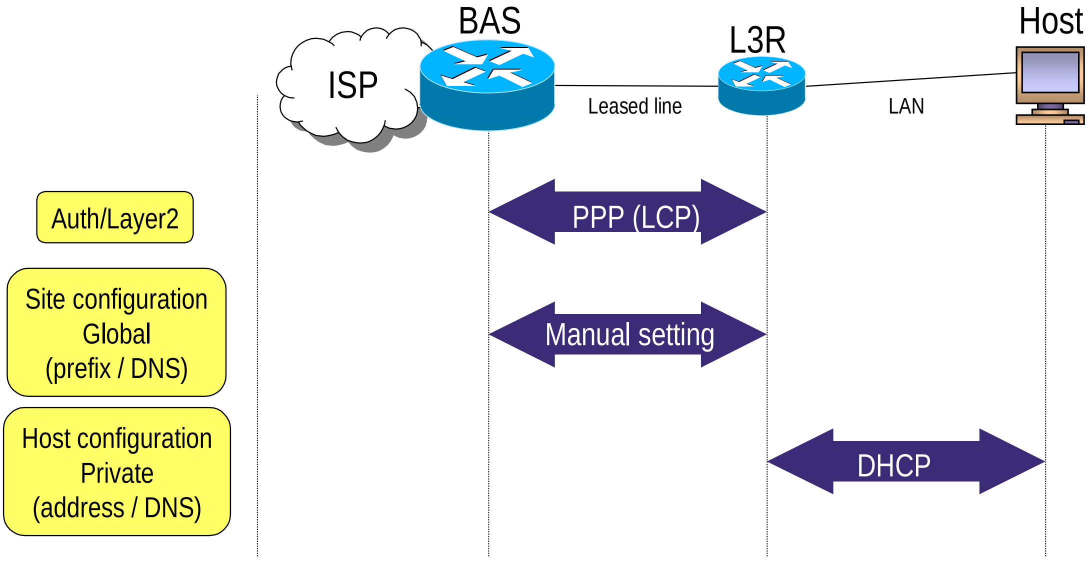
6.6.2 IPv4 Model

IPv4 model (2 types)

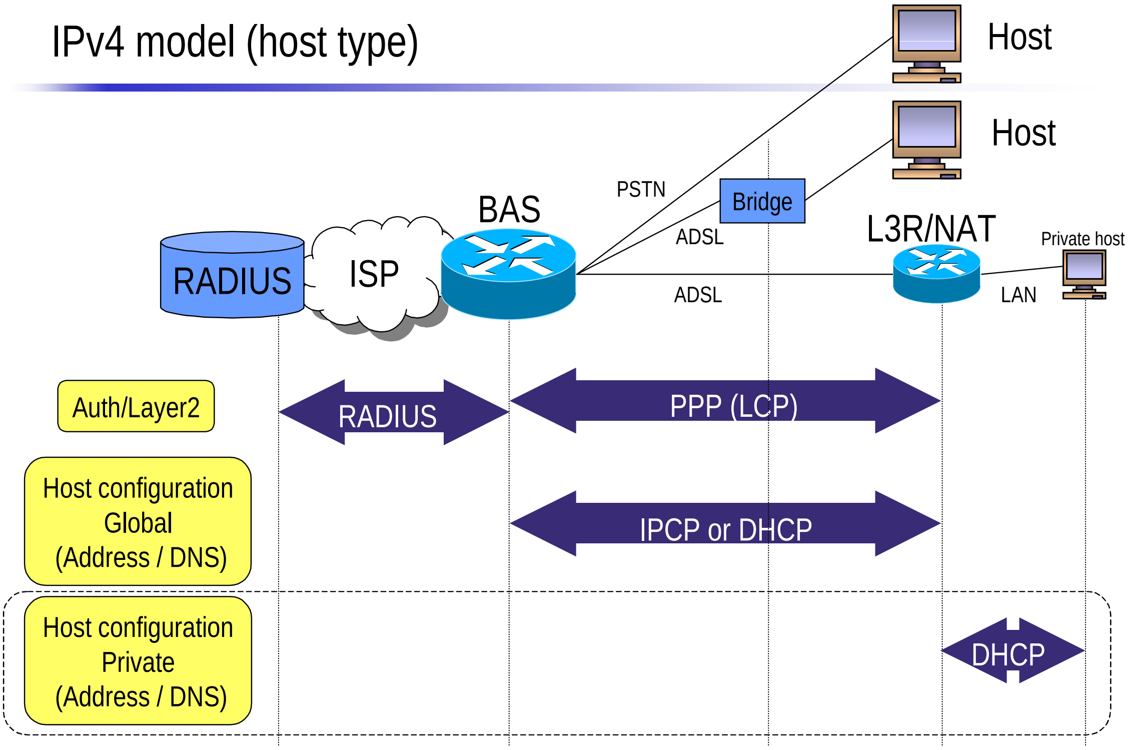


	Type of CPE	Example
Site type	L3R (router)	Economy type service, enterprise only leased line type service
Host type	L2 Bridge / none	Dialup connection type service, most ADSL/FTTH services are of this model (host = NAT / router), hotspot

IPv4 model (site type)

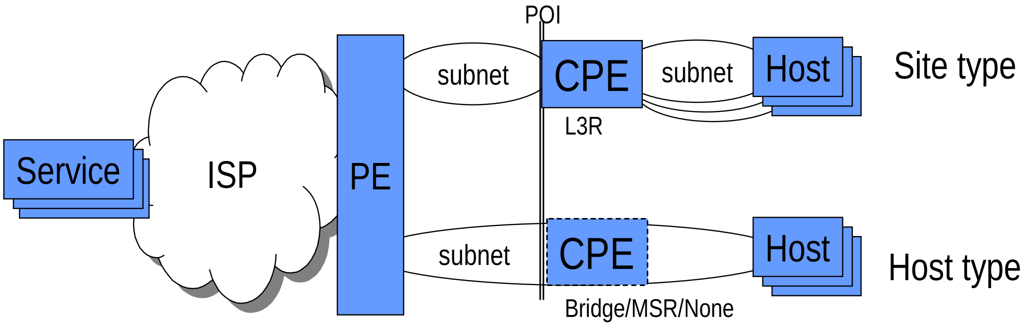


IPv4 model (host type)



6.6.3 IPv6 Model

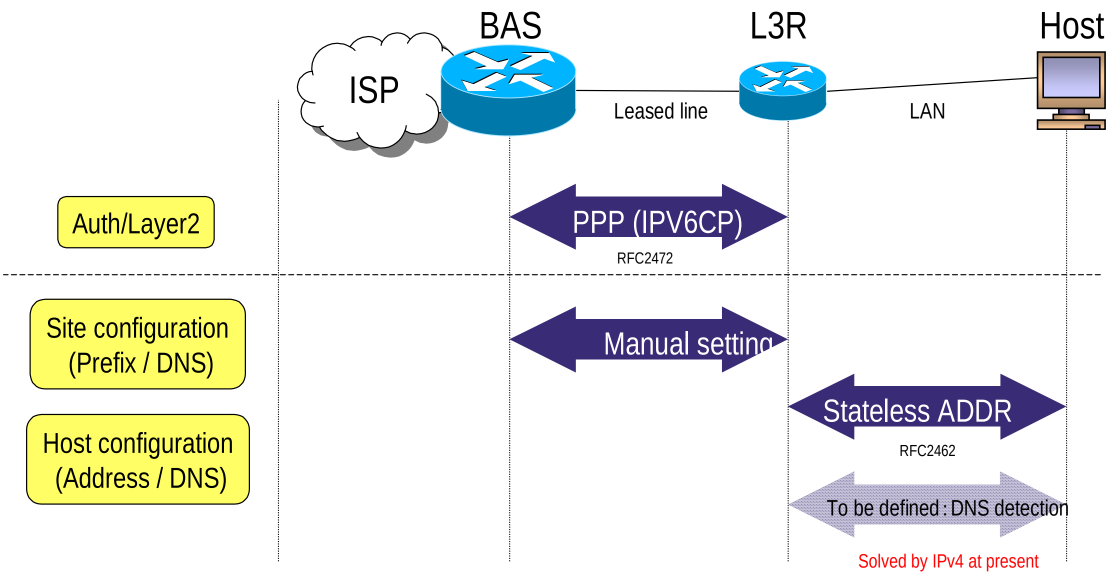
IPv6 model (2 types)



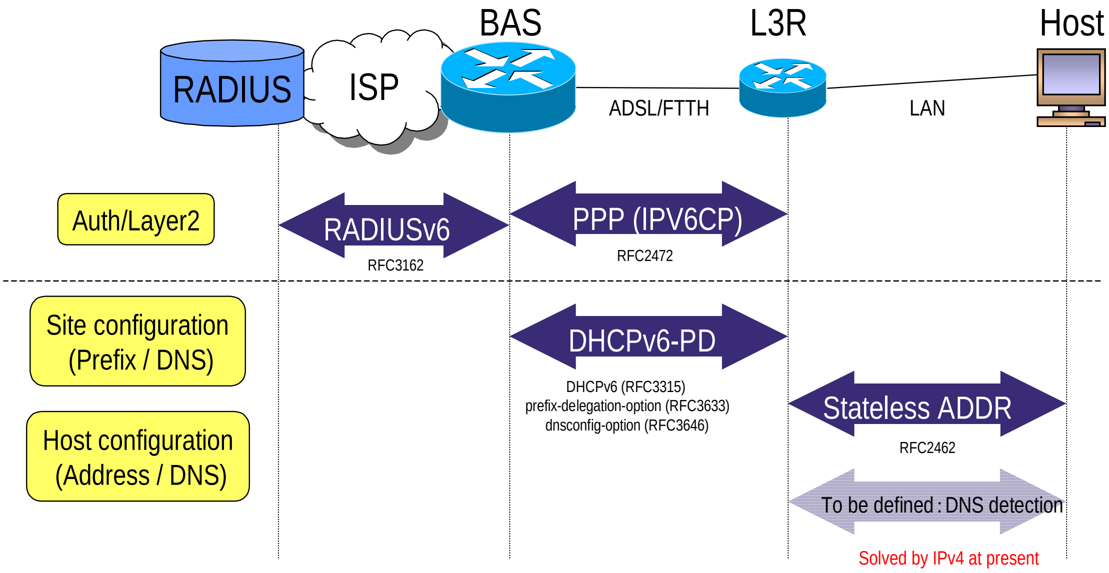
	Type of CPE	Prefix	Example
Site type	L3R (Router)	/48,/64	Enterprise only leased line type service, ADSL/FTTH service
Host type	L2 bridge/MSR/none	/64	Dialup connection type service, 3G mobile data service, ADSL/FTTH service (/64 only), hotspot

MSR=Multi-link Subnet Router

IPv6 model (site type 1)

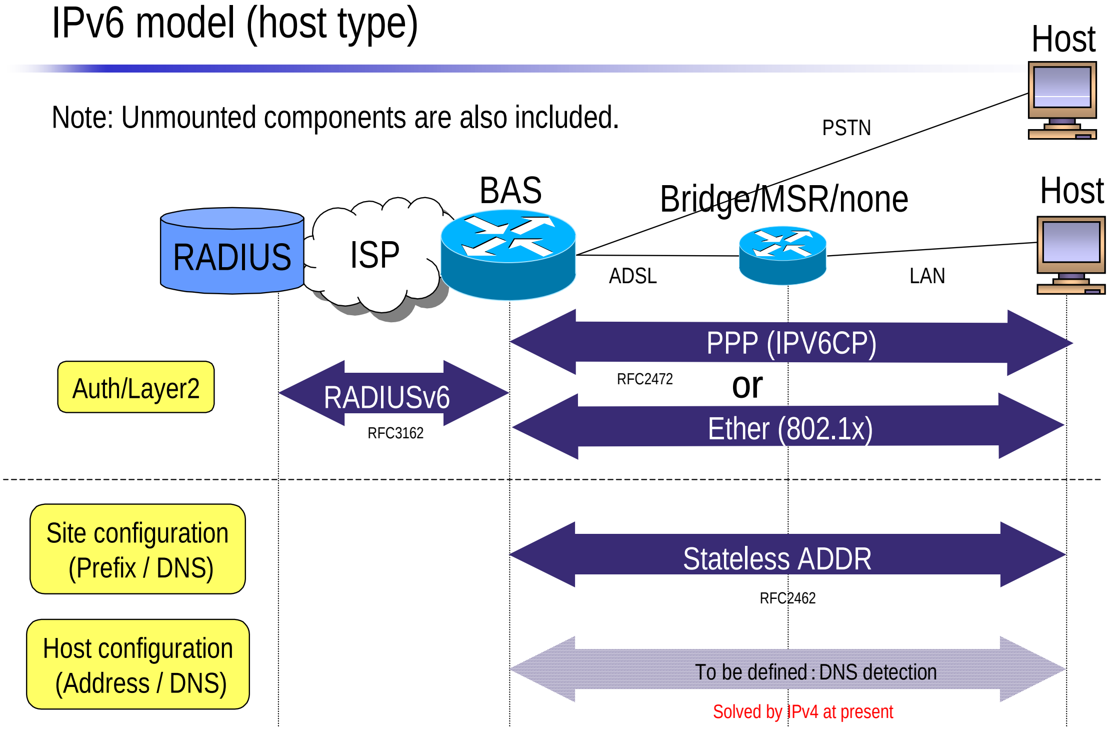

BAS
L3R
Host
ISP
Leased line
LAN
Auth/Layer2
PPP (IPV6CP)
RFC2472
Site configuration (Prefix / DNS)
Manual setting
Host configuration (Address / DNS)
Stateless ADDR
RFC2462
To be defined : DNS detection
Solved by IPv4 at present

IPv6 model (site type 2)

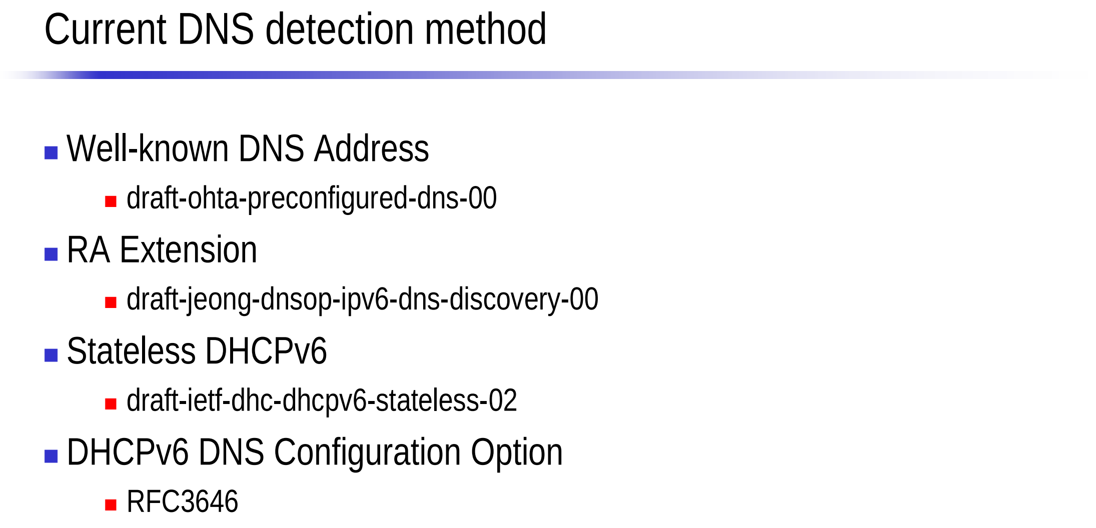

BAS
L3R
Host
RADIUS
ISP
ADSL/FTTH
LAN
Auth/Layer2
RADIUSv6
RFC3162
PPP (IPV6CP)
RFC2472
Site configuration (Prefix / DNS)
DHCPv6-PD
DHCPv6 (RFC3315)
prefix-delegation-option (RFC3633)
dnsconfig-option (RFC3646)
Host configuration (Address / DNS)
Stateless ADDR
RFC2462
To be defined : DNS detection
Solved by IPv4 at present

IPv6 model (host type)

Note: Unmounted components are also included.



6.6.4 Current DNS Detection Method



Current DNS detection method

- Well-known DNS Address
    - draft-ohta-preconfigured-dns-00
- RA Extension
    - draft-jeong-dnsop-ipv6-dns-discovery-00
- Stateless DHCPv6
    - draft-ietf-dhc-dhcpv6-stateless-02
- DHCPv6 DNS Configuration Option
    - RFC3646

"IPv6 Deployment Guideline" Based on MIC Empirical Experiments in IPv6 Deployment

＜DRAFT＞

June 2004

Ministry of Internal Affairs and Communications

Table of Contents

1. Purpose of Part 2

Ever since the term "IPv6" was first used in the IT Strategy Headquarter in 2000, the e-Japan Strategy or other areas, IPv6 has been referred to as one of the key technologies supporting IT from now on. Migrating from the current IPv4 to the new IPv6 will not just solve the problem of IPv4 addresses running out, IPv6 will carry great significance in a wide range of activities, such as allowing the networking of not only computers but also mobile phones, home appliances, automobiles and other equipment; enabling a variety of communications as required between people, between people and devices, and between devices; and providing improvements in security and communications quality to suit various utilization scenarios. The adoption of IPv6 will have an immeasurable impact on society.

Part 2 was created from the results and know-how obtained from empirical experiments in conducting migrations in actual use environments, and its aim is to assist the smooth migration from IPv4 to IPv6 in the Internet that has grown to become a basic social infrastructure today and to realize the full potential that IPv6 offers.

The environments (segments) for IPv6 deployment that are covered in Part 2 are local governments, large enterprises, small and medium-size enterprises, households, wireless LAN access environments, and ISPs. The target readers for each segment are defined in the section for each segment that follows Chapter 2 below.

■ Inquiries

For questions related to Part 2, please send email to the following address:
v6trans@ntt.com

2. Guideline for Local Government Segment

2.1 Outline

2.1.1 Aim of this Guideline

Part 2 of the Guideline contains basic information related to IPv6 deployment. It is based on a consideration for universality and assumes the general networks of local government. The aim of Part 2 is to clarify general items, policies, and methods that should be studied to ensure smooth IPv6 deployment. Part 2 also introduces the environments of actual model cases of typical local government networks. Based on these cases, Part 2 indicates specific settings that were implemented when these environments were changed to IPv6 following a number of IPv6 deployment methods. Part 2 then identifies the advantages of the deployment as well as issues and points of caution based on evaluation results for each deployment method that was actually verified.

In migrating local government networks to IPv6, a variety of cases has been assumed such as the existing network configuration, network management, policies concerning security, and cost restrictions. Part 2 introduces multiple IPv6 deployment scenarios so that network administrators can choose the most appropriate IPv6 deployment method for the various conditions in the network environment. Part 2 describes the special features and important points of each IPv6 deployment scenario, in order to facilitate efficient and effective implementation of IPv6.

Part 2 has been written mainly for personnel engaged in the construction, operation, and administration of local government network systems and for systems integrators (SIs). Although Part 2 is aimed mainly at all types of government bodies at prefectural or local levels, a large portion of the know-how in Part 2 could also be applied to networks administered by large educational institutions or general companies

2.1.2 Typical Deployment Scenarios of Local Government Networks

For typical deployment scenarios of local government networks, we refer to descriptions in deployment guidelines prepared by the Deployment Working Group of the IPv6 Promotion Council of Japan (hereafter referred to as the DP-WG).

For instance, if we assume that the entire network environment will be newly constructed, issues and problems associated with constructing the basic network need to be solved, and there are no constraints concerning issues such as compatibility with systems providing existing services. Part 2 assumes the need to migrate existing IPv4 services to IPv6 so that these services can continue to operate.

In migrating the network environment from IPv4 to IPv6, existing IPv4 services will be able to co-exist with new IPv6 services, resulting in a highly practical, flexible migration to IPv6.

It is possible to think of multiple deployment scenarios depending on environmental conditions such as desired services, functions, quality, and costs. These specific deployment scenarios are not ideally applicable in all situations. Part 2 describes a number of deployment scenarios and their features that would be applicable to a large number of situations, so that the user can choose the deployment scenario that is more appropriate for a variety of environmental conditions.

Evaluations and studies concerning cost are indispensable in building practical networks. These deployment guidelines recommend deployment scenarios based on conditions surrounding currently available IPv6-compliant products and services, and deployment costs are based on the most objective and realistic considerations possible.

2.1.3 Outline of IPv6 Deployment

Generally, if the functions of an existing network environment are being expanded, the two approaches indicated below are possible:

(a) Functions can be expanded by replacing or adding sections of hardware and software to the existing network currently being operated;

(b) Deploy a new, independent network environment without becoming concerned about constraints of the existing network environment.

If a relatively large-scale network infrastructure has already been built and effective use of the legacy network system, including cost constraints, is to be the primary focus, option (a) would be selected for most of these cases. However, if use of the network system is relatively late, or if extremely important services need to be made possible through the existing network, and especially if impact on the existing network should be avoided, option (b) would be selected for most of these cases.

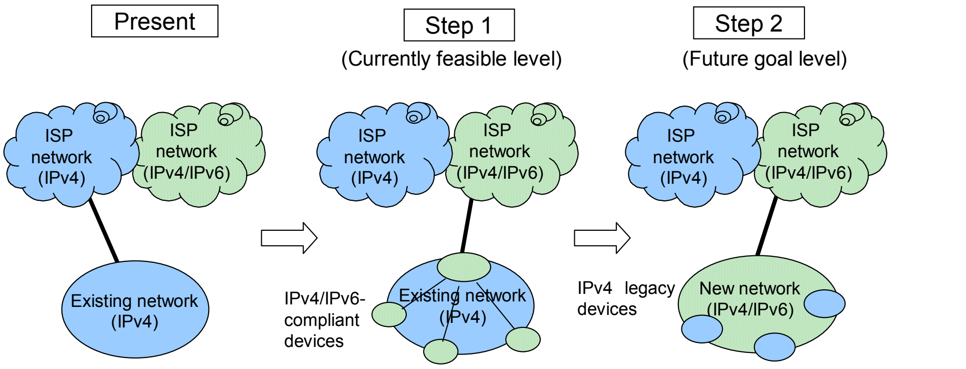
In mentioning IPv6 deployment for local government networks, Part 2 assumes the following two IPv6 deployment patterns based on both options (a) and (b) described above.

- Staged replacement (assuming cases for option (a) above)
- Independent merging (assuming cases for option (b) above)

Below, we describe each of the IPv6 deployment patterns.

Staged Replacement

The flow for the staged replacement pattern of IPv6 migration is illustrated in Figure 2.1.3.1.



- Portion of existing IPv4 network is gradually replaced by IPv6-compliant devices.
- Migration from IPv4 to IPv6 advances.
- IPv4 legacy equipment remains.

* A portion of the figure is quoted from "IPv6 Deployment Guideline (Large Enterprise / Local Government Segment)" under preparation by the Deployment Working Group of the IPv6 Promotion Council of Japan.

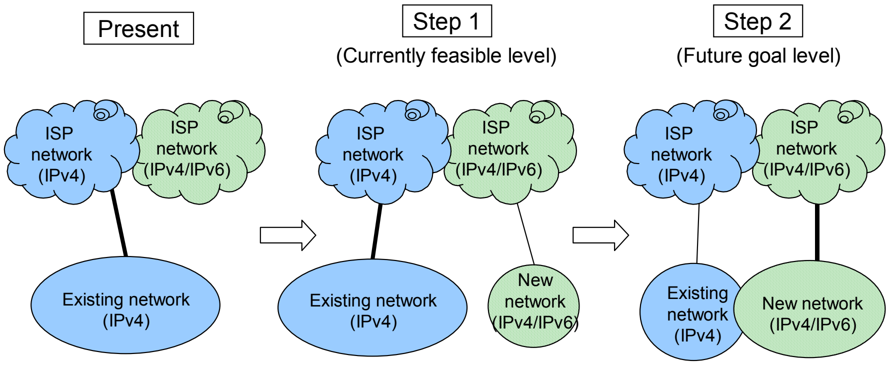
Figure 2.1.3.1: Flow for the Staged Replacement Pattern of IPv6 Deployment

In the staged replacement pattern of IPv6 deployment, the existing network is gradually migrated to IPv6 compliancy when devices undergo regularly-scheduled maintenance or replacement work. In the initial stage, a number of IPv6-compliant devices are present in the existing IPv4 network, and IPv6 are either not possible or an IPv6-over-IPv4 tunnel is configured to allow partial IPv6 access (Step 1). As replacement work toward IPv6-compliant devices progresses, the situation reverses and a number of devices not yet compliant with IPv6, such as legacy devices where IPv6 compliance is difficult, are present in the mostly IPv6-compliant network (Step 2).

In the case of staged replacement, to implement IPv6 deployment for direct existing networks, when deploying IPv6-compliant devices, it is important to ensure it does not affect existing services, such as stopping or degrading the service.

Independent Merging

The flow for the independent merging pattern of IPv6 migration is illustrated in Figure 2.1.3.2.



- IPv4/IPv6 network is built independently of the existing IPv4 network.

- Existing IPv4 network and new IPv4/IPv6 network are merged.
- Migrates gradually to mainly new IPv4/IPv6 network.

* A portion of the figure is quoted from "IPv6 Deployment Guideline (Large Enterprise / Local Government Segment)" under preparation by the Deployment Working Group of the IPv6 Promotion Council of Japan.

Figure 2.1.3.2: Flow for the Independent Merging Pattern of IPv6 Deployment

In the independent merging pattern of IPv6 deployment, a new network of IPv6-compliant devices is built independently of the existing network, and later the new network is connected to the existing network and merged with it. In the initial stage, a small-scale IPv6-compliant network is formed independently as a trial, and by having it bear no un-assumed impact on the existing IPv4 network, trial implementations concerning IPv6 can be conducted in the process of gradually building a network configuration that can achieve actual operation (Step 1). Once sufficient verification concerning the IPv6-compliant network has been completed, it is interconnected with the existing network and gradually the network migrates to becoming a mainly IPv6 compliant network (Step 2).

In the case of the independent merging pattern, since a network that is independent of the currently active network is built in the initial stage, and while the impact on existing services can be minimized, the cost of this process is higher due to the need to supply individual IPv6-compliant devices that are temporarily not used in actual operation.

2.2 Local Government Network Model

Network systems operated by local governments exist in various forms depending on the applications that these governments use them for. A feature of local government networks is that they are often separated into internal networks to support a variety of local government business services. Local government networks can be roughly classified into the following two types:

- General business networks
- Personal information networks

General business networks are connected to the Internet so that local government workers can access mail or Web sites, or publish information on local government services on their own Web site. Personal information networks, on the other hand, are for handling information in the unique possession of the local government, and since this information requires strict management, it is physically separate from other network systems that are connected to the Internet; in principle, these networks are configured independently for specific uses.

The guideline in Part 2 is aimed mainly at the general business networks mentioned above.

2.2.1 Basic Configuration of Local Government Networks

In introducing IPv6 to local government networks, we are assuming that the basic configuration of existing networks at local governments are as shown in Figure 2.2.1.1 below (prior to IPv6 introduction).

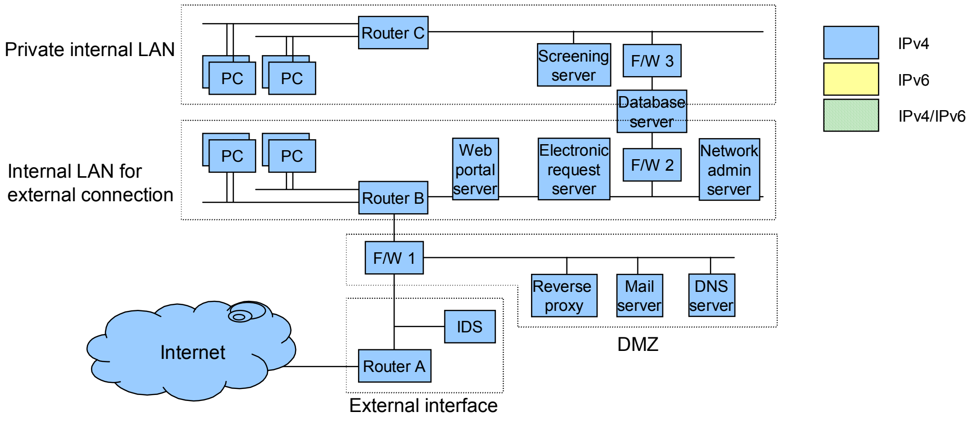


Figure 2.2.1.1: Basic Configuration of Existing Local Government Networks (Prior to IPv6 Introduction)

This local government network configuration comprises four components: an external interface section, a DMZ (DeMilitarized Zone), an internal LAN for external connection (to the Internet, etc.), and a private internal LAN. This network configuration is described in more detail below:

(1) External Interface Section

The external interface section is the section that connects the local government network directly to the Internet. It includes Router A (a router for external connection), an IDS and other devices, and is connected through a firewall to the DMZ and the internal LAN for external connection. The external interface section also includes a modem (an ONU or cable modem) for an external line.

Though many local governments use a leased always-on line of a few Mbps to 10 Mbps for their external connection line, some local governments use lines that are faster than 10 Mbps, such as IP-VPN or wide-area LAN, or regional cable Internet. These external connection lines terminate at a medium-scale router that supports WAN line capacity and is connected with the internal network. Most local governments use an IDS, but their IDS is not necessarily installed in the external interface section. Depending on where they want to detect unauthorized access, besides cases where network IDS are connected around other firewalls (at connections with the DMZ or the internal LAN for external connection), host-type

ISDs are sometimes used in the various servers.

(2) DMZ

The DMZ is an area that is separated from the internal network by a firewall and is where the servers that can be directly accessed from an external network are installed. Thus even if in the unlikely event that security measures are breached by a variety of assumed unauthorized access from outside, it is possible to prevent damage from being extended directly to the internal LAN. Various kinds of servers, such as a reverse proxy, mail server and a DNS server, are normally installed in the DMZ for disclosing services to the public via the external Internet.

(3) Internal LAN for External Connection

The internal LAN for external connection is the area that contains various servers that local governments use to provide their services to residents (the Web portal server, electronic request server, etc.) and the various PCs that local government workers use to connect to the Internet using Router B (a large router or L3 switch).

For these servers to provide these services on the Internet, and in order to avoid direct access from outside, the access is channeled through the reverse proxy server installed in the DMZ. This not only allows a cache function to be used to lighten the load of the various servers (the Web server, etc.) but it also has the security advantage of preventing the server main units from being exposed to the outside. Regarding public servers such as the Web server in particular, on relatively small networks, it is common for public servers to be installed directly in the DMZ without requiring access through a reverse proxy, or for a Web hosting service to be used and subcontract Web server administration to an ISP or other enterprise.

In the example of the server cluster in this configuration, there are a Web server and an electronic request server, and all access with the outside is passed through the reverse proxy. The electronic request server shown here is given as an example of a legacy application providing existing services. The Web portal server is given as an example of an application built into the system on the base of an application program that is universally used.

There are cases in which the number of PCs used by workers reaches several hundred, depending on the scale of the local government. It is possible that they have a large-scale network environment that is divided into a number of segments according to the configuration or size of the organization or the building. If a general PC on the local government network is accessing the Internet, the access is limited to the minimum possible. For example, it is normal for Web (HTTP) access to the outside to also be passed through the proxy server (doubling as the "Reverse proxy" in Figure 2.2.1.1). The example of the configuration in this figure shows the smallest scale possible.

(4) Private Internal LAN

The private internal LAN is a network configured independently of the internal LAN for external connection. It is a network segment that is not directly connected to the Internet.

Besides the internal LAN connected to the Internet, local government networks often have network systems, such as LG-WAN or basic residential registers network, that focus on the privacy of personal or corporate information. Here we refer to all of these networks as private internal LANs.

The database servers that are shared by the private internal LAN and the internal LAN for external connection are not only set so that they do not allow information to be transferred between the two LANs, they also have firewalls that boost their independence.

2.2.2 Redundant Configurations

Some local government networks have adopted some sort of redundant configuration measure for the main units on the network out of consideration for the reliability or safety of their services. For example, dynamic routing can be applied by double-layering the backbone router. Even if a redundant configuration is not adopted, measures for specific equipment, such as preparing a spare unit, have been adopted so that quick manual switching is possible in the event of a malfunction.

It is assumed that there is little need at the initial IPv6 deployment stage for a redundant configuration in the IPv6 network configuration that is the target of Part 2, and is therefore not discussed. The redundant configuration has also been omitted in the assumed existing network configurations due to considerations for universality.

2.3 IPv6 Deployment Policies

Here we describe basic philosophies concerning IPv6 deployment on local government networks.

2.3.1 Overall Policies Concerning IPv6 Deployment

(1) Introduction Objectives

From a short-term, local perspective, it is not impossible to provide various services that utilize IP phones, IM or other features in addition to Web access or mail on an existing IPv4 network infrastructure without introducing IPv6. Most of the various application services based on IPv4 in its current situation, however, are provided after various added measures have been incorporated due to constraints on such items as address space, address management, and packet format. Accordingly, if sophisticated network services on the Internet including authentication for each individual user and security management are introduced on an IPv4 base from now on, the network system will become extremely complex and the introduction costs and operation and administration costs will become prohibitive. The longer the delay in switching from IPv4 to IPv6, the greater the impact from these problems will be.

Besides offering an address space that is dramatically larger than that of IPv4, since IPv6 is a new Internet protocol that compensates for the weaknesses of IPv4 thus far, it facilitates smooth use of end-to-end communications, sophisticated security communications, mobile communications and other communications whose use is expected to expand from now on. Networks operated by local governments need to allow high security management of personal and corporate information and offer user-friendly network environments so that a wider range of residents can use the Internet. In order to provide more local government services over the Internet from now on, the deployment of IPv6 is essential. If migration to IPv6 is also to consider maintaining existing network services, the migration cannot occur as quickly as one might think. New local government services can be offered in the future only by gradually switching the network infrastructure base from IPv4 to IPv6 starting at an early stage.

(2) Impact on Existing IPv4 Network Services

Since IPv4 and IPv6 are originally separate, incompatible protocols, network equipment that supports only IPv6 will not be able to process IPv4. Also, since IPv4 and IPv6 operate independently as a function of layer 3 (the network layer), basically they can coexist on the same network infrastructure. In layer 2 (the data link layer) and below, however, since the same network resources (mainly Ethernet) are shared, study and management concerning traffic volume are required, and the impact of IPv6 deployment on IPv4 needs to be considered.

Local government networks are used for their own internal local government work or for providing services to local residents, and through specially incorporated designs, tend to use service applications with relatively low universality for a long time. It is thought that a large number of these types of applications has already been introduced on the IPv4 base, and if this is so, it would be difficult to migrate them completely to IPv6. To proceed with IPv6 migration in local government networks, if services utilizing the existing IPv4 network are to be continued especially in the initial stage, in principle, a dual stack network system capable of running IPv4 applications as is should be built.

In services that utilize the DNS name resolution function, since the introduction of IPv6 may indirectly extend an adverse impact on IPv4 services (see "IPv6 Server DNS Registration" for details), serious study and evaluation/confirmation work needs to be performed when building the dual stack network.

(3) Range of Application

In the initial stage, the basic approach to deploying IPv6 is to update the network infrastructure so that services that are being provided on the IPv4 network can also be provided on IPv6. Accordingly, it is possible for the overall network infrastructure that is currently running on IPv4 to migrate within the range in which IPv6 is to be applied. However, the purpose of deploying IPv6 is not just to migrate to IPv6 but to provide new network services in the future. Since this is the purpose of building a network infrastructure, the range in which IPv6 deployment is to occur needs to be narrowed down and clarified based on a consideration of this purpose.

In local government networks in particular, it is possible that in many cases networks of many types exist independently according to their application or the level of security required. In this sort of network environment, the general work network that is connected to the Internet is the first network to be migrated to IPv6. Networks that are independent of the Internet should also be migrated to IPv6 if in the future the purpose of their use requires a higher level of security and it is hoped that this network infrastructure will be connected to the Internet.

(4) Introduction and Administration Costs

Though the costs of hardware and software network elements do not rise significantly even if they support IPv6 in addition to IPv4, at the initial stage of IPv6 introduction, network management for both IPv4 and IPv6 is required, causing the burden of cost to rise. Two major negatives in particular are that the IPv6 network is not as practical or refined for providing services as IPv4 and that only a few network administrators or systems integrators are experienced or knowledgeable in IPv6.

In the future, however, new services will be introduced on the IPv6 base, and when existing services are expanded, they too will support IPv6, so that eventually most network services will be integrated from IPv4 into IPv6. Thus, the costs for continuing to maintain the IPv4 network and the disadvantages of IPv4's technical constraints are expected to rise dramatically over time.

(5) Security

Services utilizing the Internet have developed dramatically in terms of the variety of fields that offer such services, the ways these services are used, and the users themselves. In local government networks, however, along with ease and convenience in using these services, they need to maintain reliable security. Since local government networks in particular handle personal and corporate information which requires solid information management, network services cannot be introduced only on the merits of their convenience. The deployment of IPv6 will not only enable encrypted communications between terminals using IPsec, for instance, it will also allow improvements in total network security in such areas as authentication and analyses of unauthorized access attempts.

There are also many cases of misunderstanding that all security measures will be infallible simply by introducing IPv6. It is naturally meaningless to introduce IPv6 unless if it does not operate correctly. At this point in time, the basic approach is to have security policies that were operating under IPv4 (such as firewalls, IDS, and virus checkers) continue to operate as is under IPv6 as well.

2.3.2 Network Security Policies in the Initial Stage of IPv6 Deployment

Local government network systems require a higher level of security compared with other network systems. By deploying IPv6, if a new application such as IP phone end-to-end communications is provided, from the perspective of relaxing allowable communication conditions in the firewall filtering settings, compared with the filtering conditions on the existing IPv4 base, the IPv6 solution under current conditions requires a certain amount of compromise in security management. Since actual problems such as these occur in the initial stage of IPv6 deployment, Part 2 introduces the following two approaches:

- Relaxed model
- Strict model

These two approaches, however, are only provisional. More concrete network security policies concerning IPv6 still need to be clarified and is a major issue that needs to be resolved as soon as possible.

(1) Relaxed Model

The relaxed model is a security model that, in making basic network security settings for the deployment of IPv6, uses the same security policies that were used in IPv4. In other words, the firewall and the various router filtering functions are all made to operate under IPv6, and IPv6 refers to the filtering settings that were used on the IPv4 base.

However, when a new application such as IP phone is introduced with IPv6, communication between terminals on the network and terminals outside the network is not possible under the existing filter settings. It is therefore necessary to relax the filter settings in the minimum required range in order to use any of the new applications. In the initial stage in particular, it is possible to independently limit segments where new applications are introduced and to relax the filter settings just for those segments. For example, the range of impact should be minimized by limiting wherever possible the segments or terminals that can be accessed, and not just relaxing the filter settings according to type of service (port numbers, etc.).

Generally, in order to realize access to the IPv6 Internet, it is possible to use IPv6-over-IPv4 tunneling. In this case, the terminal section of the tunnel becomes the DMZ or a new network segment that was secured separately, and security should be obtained by completely shutting down connectivity with the existing IPv4 internal network.

(2) Strict Model

Even if IPv6 were made to co-exist in the existing IPv4 network, by setting IPv6 security settings to the existing (IPv4) equivalent settings, it is possible the network for practical purposes will operate without problem. Depending on standards of the local government's particular network security settings, it is possible that unforeseen dangers may appear, and there may be cases where the introduction of IP applications on the existing network being operated will need to be delayed. The security model that is applied in these types of cases is known as the strict model. In the strict model, a new IPv6 network is built independently of the existing network, and security settings that are independent of the existing network are established.

The IPv6 deployment pattern based on this sort of strict model corresponds to the initial stage of the independent merging pattern. Since new networks in the independent merging pattern are physically independent of the existing network, they have no impact on the security of the existing network. In new networks, the most appropriate security settings can be found by relaxing applicable security settings in the trial stage, verifying the use of a variety of applications, and verifying and evaluating the effectiveness of the security over time.

2.4 Elemental Technologies for IPv6 Deployment

Three elemental technologies for IPv6 deployment are given below:

- Tunneling (IPv6-over-IPv4)
  This technology allows IPv6 terminals to communicate with each other through network segments that do not yet support IPv6 by encapsulating the IPv6 packets in an IPv4 packet and transferring it through those segments.
- Protocol Translation (NAT-PT, TRT, Proxy-type protocol conversion, etc.)
  This technology interpositions a function between an IPv4 terminal and an IPv6 terminal that converts IPv4 and IPv6 protocols so that terminals with different protocols can engage in direct communications virtually.
- Dual Stack
  This technology supports both IPv4 and IPv6 protocols and allows IPv4 terminals or IPv6 terminals to directly communicate with each other over the same line.

A brief description of the features of these elemental technologies is provided below:

2.4.1 Tunneling

Tunneling (IPv6-over-IPv4) technology allows IPv6 terminals to communicate with each other through network segments that do not yet support IPv6. To achieve this, this technology encapsulates the IPv6 packets in an IPv4 packet and transfers it through those segments. An overview of an IPv6 migration method that uses tunneling is shown in Figure 2.4.1.1.

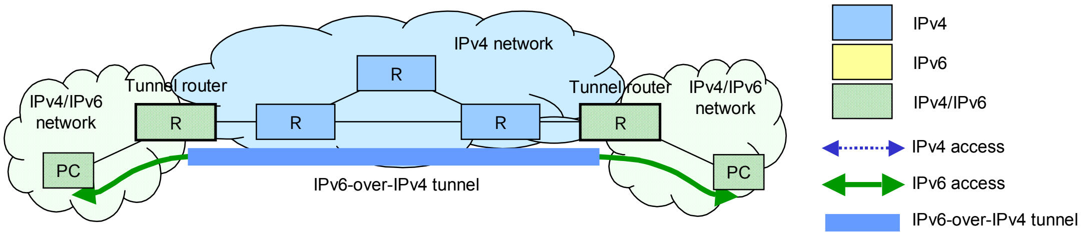


Figure 2.4.1.1: Overview of an IPv6 Deployment Method that Uses Tunneling

An IPv6-over-IPv4 tunnel can be used to secure IPv6 accessibility on an IPv4 network by installing IPv6-compliant equipment in certain sections. Conversely, IPv4-over-IPv6 tunneling could be used to secure IPv4 accessibility on an IPv6 network by leaving IPv4-compliant equipment in some sections, but for the time being, it is believed this will not have any practical operation.

The main advantages of Tunneling, an effective provisional approach for the initial stage of IPv6 deployment, are as follows:

- IPv6 accessibility can be provided simply by installing IPv6 devices in certain sections of the network.
- No special awareness of tunneling is required other than by the device at the terminating end of the tunnel.

The main disadvantages of Tunneling are as follows:

- In the control of IPv4 packet routing through the tunnel, all tunnel packets (protocol No. 41) are treated in the same way even when multiple communication applications are present at the same time.
- Packet transfer efficiency is worse due to the longer length of encapsulated packets.
- Encapsulated packets that are longer than the Maximum Transmission Unit (MTU) when they are passing through IPv4 network segments, if a fragmentation prohibit flag is active, will be abandoned (see "MTU (Maximum Transmission Unit)" for details).

2.4.2 Translation

The main uses of the IPv4/IPv6 translation function using a translator or proxy in local government networks are shown in Figure 2.4.2.1.

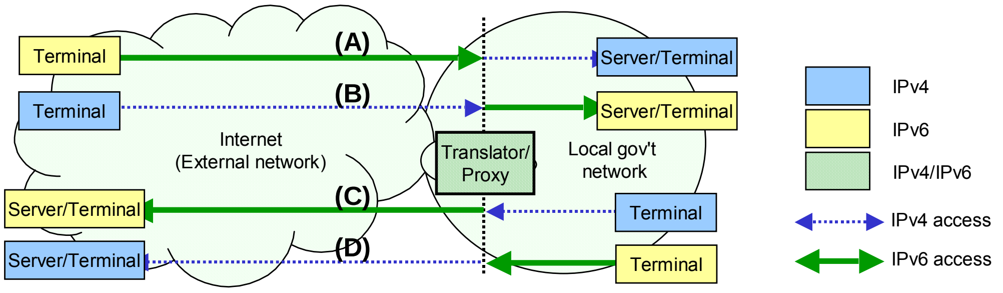


Figure 2.4.2.1: Main Uses of the IPv4/IPv6 Translation Function

(A) represents the case in which an external user terminal that was the earliest to support IPv6 accesses a non-IPv6-compliant server or other device on the local government's internal network, and is a case that is believed to have the potential of occurring[1].

(B) represents the case in which an external user terminal that does not support IPv6 accesses a server or other device on a local government's internal network that supports only IPv6, but this case is not thought to have the potential of occurring if the local government network is migrated for the purpose of IPv4/IPv6 dual stacking.

(C) represents the case in which a user terminal on a local government's non-IPv6-compliant internal network accesses an external server that supports only IPv6 or a server or other device that can provide additional services if they are IPv6, and is a case that is believed to have the potential of occurring.

(D) represents the case in which a user terminal on a local government's internal network that was the earliest to support IPv6 accesses a non-IPv6-compliant external server or other device, but like case (B), this case is not thought to have the potential of occurring if the local government network is migrated for the purpose of IPv4/IPv6 dual stacking.

As shown above, for IPv4/IPv6 translation to be used on a local government or other user network, primary consideration should be placed on translation that is used for (A) and (C) at the minimum, in other words, for bi-directional translation between external IPv6 communications and local government internal IPv4 communications.

Though a number of translation (IPv4/IPv6 protocol conversion) systems has been proposed thus far, considering their practical use on the level of a working product,

[1] Windows XP and others give priority to IPv6-based access.

the two types below are the main ones of influence:

- NAT-PT, TRT --> Translator
- Proxy-type protocol conversion --> Proxy

A device equipped with a NAT-PT (Network Address Translator – Protocol Translator) and a TRT (Transport Relay Translator) are generally called a "translator" and are used for translation. Also, a device equipped with a proxy-type protocol conversion function is simply called a "proxy" Below, we briefly describe the features of a translator and a proxy.

Translator (NAT-PT, TRT, etc.)

An overview of an IPv6 deployment system that uses a translator is illustrated in Figure 2.4.2.2.

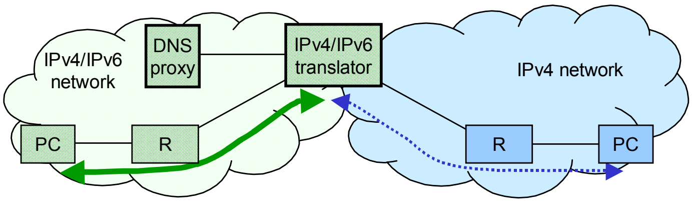


Figure 2.4.2.2: Overview of IPv6 Deployment System Using a Translator

When a translator is used, an IPv4 terminal and IPv6 terminal can directly communicate with each other virtually. The translator is linked to the DNS proxy, and when a virtual IPv6 address for the IPv4 terminal and a virtual IPv4 address for the IPv6 terminal are automatically generated for the domain name, as a relay device, the translator converts the IPv4/IPv6 protocol, allowing communication to take place between different protocols without the IPv4 terminal or IPv6 terminal becoming aware of the protocol conversion.

A translator is different from a proxy in that, at the time of protocol conversion, the addresses of both the destination and the origin are converted to support the original address of each terminal.

The main advantages of the translator, an effective approach for local government networks that have a large number of systems (legacy systems) that have difficulty in directly supporting IPv6, are as follows:

- By simply installing IPv6 devices in certain sections of the network, devices and systems that do not actually support IPv6 can be accessed virtually from outside as if they are IPv6-compliant.
- If domain names are registered in the DNS, communication is possible by linking with the DNS proxy and automatically generating a random virtual IP address for a connection destination that is of a different protocol (IPv4/IPv6).
- All communication terminals do not especially need to be aware of protocol conversions.
- Protocol conversion takes place at layer 3 (NAT-PT) or layer 4 (TRT), and processing speed is relatively fast despite the low layer where processing occurs.

The main disadvantages of the translator are as follows:

- Not applicable with some applications. (Since support for simple protocol conversion at the network layer [L3] is not always possible, ALG [Application Level Gateway][2] or similar is required if SIP or other IP address information is used at a higher layer.)
- Automatic protocol conversion by the DNS cannot be applied for communication terminals without a domain name.

[2] Communication data is processed up to the application layer and then transferred. The proxy can be considered the ALG of the Web application.

Proxy

An overview of an IPv6 deployment system that uses a proxy is illustrated in Figure 2.4.2.3.

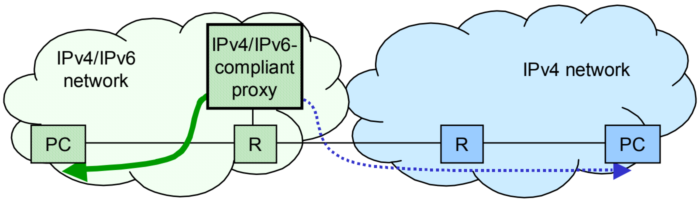


Figure 2.4.2.3: Overview of IPv6 Deployment System Using a Proxy

Depending on how it is used, a proxy is either called a proxy (acting as an agent for the access terminal) or a reverse proxy (acting as an agent for a public server). Basically, like a translator, a proxy is used to enable an IPv4 terminal and an IPv6 terminal to directly communicate with each other through a virtual process. As an agent of a specific server, a proxy relays access to the server. Its main original purposes are as follows:

- To strengthen security by checking packet content when relayed on the Internet.
- To enhance speed by storing content in cache memory.

By equipping this proxy with an IPv4/IPv6 protocol conversion function, an IPv4 terminal and an IPv6 terminal can communicate with each other over different protocols.

Unlike a translator, a proxy is positioned between the sender and the recipient during protocol conversion, and the proxy itself assumes the communication between the two parties.

The advantages of a proxy are as follows:

- Virtual IPv6 support is possible for non-IPv6-compliant devices and systems that want to communicate with external terminals.
- All communication terminals do not especially need to be aware of protocol conversions.
- It is possible to equip each application with unique added functions.

A disadvantage of a proxy is as follows:

- The number of applications to which a proxy can be applied is limited.

2.4.3 Dual Stacks

An overview of an IPv6 deployment system that uses a dual stack is illustrated in Figure 2.4.3.1.

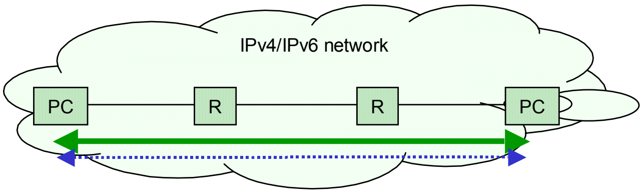


Figure 2.4.3.1: Overview of IPv6 Deployment System Using a Dual Stack

When a network is configured with dual stacks, native access without converting all communication packets is possible. In the initial stage of IPv6 introduction in particular, it is difficult to build and operate a native IPv6 environment that does not use IPv4 at all. Since the dual stack configuration allows communications to occur in either IPv4 or IPv6, it is possible to gradually migrate applications to an IPv6 base while operating both protocols. A network environment with a high level of freedom is possible with dual stacking.

The advantages of dual stacking, an ideal approach to IPv6 deployment in the initial stage, are as follows:

- Since no special conversion functions are used, there are few constraints on using IPv6 and operation of the network can take advantage of the original features of IPv6.
- Since IPv4 can also be used in the same way, there are few constraints in migrating to IPv6.

A disadvantage of dual stacking is as follows:

- The cost of introducing and operating these devices is a disadvantage.

2.5 IPv6 Deployment Scenarios

Since a variety of environment conditions is possible in local government networks, it is not possible to decide on a single scenario for IPv6 deployment. In this section, we present a number of IPv6 deployment scenarios that serve as guidelines that should be referred to when carrying out standard IPv6 deployment.

2.5.1 Applying IPv6 Deployment Technologies

Basic approaches to applying the various IPv6 deployment technologies to local government networks are given below.

(1) Tunneling

The maintenance of security policies needs to be considered when applying tunneling to local government networks. Since current firewalls cannot implement checks on the information contained in packets that have been encapsulated through tunneling, a policy to address this shortcoming is required. For example, if 6to4 tunneling can be used to establish a direct tunnel between a 6to4 relay router on the Internet and a terminal on the local government's internal network, and since the security functions present at the borders of the local government network would then become meaningless, the firewall at the borders should prohibit the passage of these sorts of tunnel packets.

Thus if tunneling is to be used in introducing IPv6, the following policies should be adopted:

(a) The IPv6-over-IPv4 tunnel shall terminate momentarily at the stage prior to the border.

(b) The firewall and other devices inside the border shall be made to support the processing of native IPv6 packets.

(c) If changing to IPv6 inside the local government is difficult, an ISATAP tunnel or other means shall be applied to configure a tunnel connection that is closed to the internal network.

(d) If support for (b) is difficult, since drawing IPv6 packets into the local government's internal network will then be dangerous, an independent IPv6 segment shall be configured at the stage prior to the border, and test operation shall be conducted.

In (a), if use is limited to test purposes, a 6to4 tunnel can also be applied in addition to applying tunnel connection services (static IPv6-over-IPv4 tunnel) that ISPs are already starting to provide. If only general services (Web access and mail access) are being used on the local government network, in migrating to IPv6 on a network connected to an ISP, there will be no great impediment if the tunnel system is used. If the ISATAP or other tunnel terminates at the terminal, however, some applications may not recognize the IPv6 interface that uses a tunnel, in which case we recommend that its use be temporarily stopped and native IPv6 deployment (using dual stack system) be carried out as soon as possible.

(2) Translator/Proxy

<The need for translation>

The use of a translator or proxy makes it technologically possible to introduce IPv6. From now on, however, it is expected that a growing number of new applications utilizing end-to-end communications will be introduced on local government networks. Since the features of these applications will be used to greatest advantage when devices can communicate directly with each other, this will be one of the primary objectives in introducing IPv6. Considering this background, even if IPv6 is introduced by having a translator or proxy convert the IPv4/IPv6 protocol, essentially this method will not be able to take sufficient advantage of the merits of IPv6. If new applications utilizing unique advantages of IPv6 are to be introduced, it is best to completely avoid using translation functions and to promote IPv4/IPv6 dual stacking instead.

Depending on individual network environment conditions, however, it might be necessary to apply translation in order to realize virtual connectivity between an IPv4 terminal and an IPv6 terminal. Specifically, this case might occur when there is a desire to make difficult legacy systems become IPv6-compliant as part of an attempt to realize total IPv6 deployment. If translators or proxies are to be used in introducing IPv6, the purposes and targets for their use should be clarified in advance, and they should be introduced in certain segments only.

<Comparison between a translator and a proxy >

In comparing a translator and a proxy, for a network usage environment like a local government network where extremely large traffic loads are rare or the number of external public servers and other devices that would require translations is limited, an IPv4/IPv6 protocol conversion system that uses a proxy is easier to install than one that uses a dedicated translation device.

On the other hand, a dedicated translator should probably be installed if there is a demand for translation from general-use applications not limited to specific users and the translation load is sometimes relatively high.

(3) Dual Stacks

Dual stack IPv6 deployment should basically be studied in all cases of IPv6 deployment. In local government networks, however, it is expected there will be difficulties, due to the scale of the networks, to make various network devices become compliant with IPv6. Although the long-term goal of the network configuration should be to dual stack the overall local government network, tunneling and translation offer realistic methods in the process of migrating to IPv6 migration.

2.5.2 Scenarios for Each IPv6 Deployment Pattern

The appropriateness of various combinations of "IPv6 Deployment Patterns" and "IPv6 Deployment Technology," based on the results of the studies and evaluations concerning IPv6 deployment given in the previous section, is summarized in Table 2.5.2.1.

Table 2.5.2.1: Appropriateness of IPv6 Deployment Technologies for Each IPv6 Deployment Pattern

IPv6 deployment technology	IPv6 Deployment Patterns			
	Staged Replacement Type		Independent Merging Type	
	Initial stage	Mature stage	Initial stage	Marging stage
Tunneling	○	—	△	—
Translator (*1)	△	△	—	△ (*2)
Proxy (*1)	△	△	—	△ (*2)
Dual stacking	○ (*3)	◎	◎	◎

(*1) Choose either translator or reverse proxy.
(*2) Existing service applications can be made to virtually support IPv6 when merged with existing network
(*3) Minimum required devices must be dual stacked.

Since the tunneling, translator, and proxy techniques are IPv6 deployment technologies that take advantage of the existing network infrastructure, their application in the staged replacement type is effective. Though the tunneling, translator, and reverse proxy techniques can be applied in the independent merging approach when merging a newly-built independent network with the existing network, it is not realistic to apply them at the initial stage.

The dual stack technique, however, is appropriate for application in the independent merging approach, as it makes all devices IPv6-compliant. Although all efforts should be taken to use dual stacking in the introduction of IPv6 in the staged replacement approach, considering the need to hold down costs, tunneling, translators, reverse proxies and other techniques can be effectively combined enhance cost effectiveness in the initial stage of migration.

IPv6 deployment scenarios for each IPv6 deployment pattern are described below.

(1) Staged replacement scenarios

The basic approach to promoting IPv6 deployment is to assume dual stacking. Considering cost constraints and other needs such as periodic maintenance and replacement of network equipment, however, in the initial stage, it is more realistic to gradually expand IPv6 accessibility by making portions of the equipment IPv6-compliant.

In responding to cost constraints, particularly at the initial stage, it is probably good to use IPv6-over-IPv4 tunneling. If trial introductions are being assumed, using a 6to4 tunnel is a low-cost way to introduce IPv6 on an ISP connection line. Due to security considerations, however, IPv6-over-IPv4 tunnels should not be drawn directly as is into the internal networks of local governments. At the section just before the firewall in the border section of the local government network, a device to first terminate the IPv6 tunnel at this point should be installed. There are many ways to terminate the tunnel, and any of the ones mentioned below can be used.

- Make existing routers IPv6-compliant.
- Add a new IPv6 (tunnel)-compliant router.
- Install a firewall that can terminate a tunnel.

An IPv6-compliant firewall should be installed as soon as possible. In the staged replacement approach, introducing IPv6 in a local government's internal network without having an IPv6-compliant firewall should be avoided due to security considerations.

When considering the minimum required IPv6 compliance for network devices in the process of introducing IPv6 in the internal networks of local governments, it is effective to tentatively use tunnels. It is possible to use ISATAP tunnels in internal networks configured of private IPv4 addresses. A problem with the OS and applications loaded in the terminal, however, is that the ISATAP interface that directly terminates the tunnel does not function effectively, sometimes preventing the ability of the terminal to use IPv6. The active promotion of ISATAP should therefore be avoided and used only as little as possible. The basic approach is to switch the default router of the network segment to be migrated to IPv6 to an IPv6 (tunnel)-compliant router, and it is probably good to make the entire network segment under the router by setting a static IPv6-over-IPv4 tunnel.

It is also possible to secure connectivity with external IPv6 terminals for devices on a local government network that are not yet IPv6 compliant by introducing IPv4/IPv6 translators or IPv6-compliant proxies. It is possible, however, that IPv6 compliance using translators or proxies may be unnecessary if native IPv6 compliance rather than substantial IPv6 deployment is the future goal. One case in which translators or proxies could be used to introduce IPv4/IPv6 protocol conversion functions on a local government network would be when IPv4-based applications specializing in each of the local government services and their legacy servers and other equipment would be relatively difficult to support IPv6 in the future.

(2) Independent merging scenarios

Basically, the dual stack system should be used to build a new network that is IPv6-compliant and independent of the existing network. Since there is a large risk in simply bringing a new IPv6 network to actual operation without conducting trials, a fixed period for verification should be secured. In the initial stage of new network introduction, functions should be verified using a minimum configuration consisting of IPv6-compliant routers and terminals. In this stage, it is possible to verify IPv6 connectivity even when applying a 6to4 tunnel or other device. After that, the goals of utilizing IPv6 become clear, and in the stage that aims for full-scale IPv6 operation, particular note should be made concerning the following points:

- Conclude a formal contract with an ISP for IPv6 line connection services.
- Check the IPv6 functions at the network borders (at firewall, IDS, etc).

Dual stacking, and not using IPv6-over-IPv4 tunneling or IPv4/IPv6 translation, should be adopted as the basic deployment policy for the network infrastructure, and all efforts should be made to build a network system on an IPv6 base.

Besides introducing basic IPv6-compliant Web, mail, and other applications, future operation and expandability supporting IPv6 should also be considered when introducing new local government service applications. IP phone and videoconferencing systems are some of the possible local government service applications.

Since it is not efficient to continue operating two types of networks, at some time in the future, the new IPv6 network should be merged with the existing network. By merging the networks, applications that had been running on the existing network are gradually migrated to the IPv6 network, and ultimately the IPv4 network environment is expected to lose its practical use.

2.6 Practical Examples of IPv6 Deployment

In this section we describe concrete examples of networks that have been built on typical bases of "IPv6 deployment technology." These examples are useful for studying IPv6 deployment in local government networks. Along with describing the methods and know-how for introducing IPv6, we indicate the features and problem areas that have occurred in these networks that have been built.

In applying the four "IPv6 deployment technologies" described above, we have organized methods for taking effective advantage of each of these deployment technologies for local government networks. We propose four "IPv6 deployment methods" below:

(a) Tunnel method

Tunneling and dual stack are used as an IPv6 deployment pattern in the staged replacement type of IPv6 deployment.

(b) Translator method

Translators and dual stack are used as an IPv6 deployment pattern in the staged replacement type of IPv6 deployment.

(c) Proxy method

Proxies and dual stack are used as an IPv6 deployment pattern in the staged replacement type of IPv6 deployment.

(d) Dual Stack method

Dual stack is used as an IPv6 deployment pattern in the independent merging type of IPv6 deployment.

These deployment methods do not necessarily need to be used independently of each other. They should be combined as needed.

2.6.1 Model Case for Local Government Networks <Prior to IPv6 Deployment>

Based on the basic configuration of a local government network shown in Figure 2.2.1.1, we introduce a model case as a concrete network example prior to IPv6 deployment. Part 2 of the Guideline uses this model case as an assumption in describing practical methods of IPv6 deployment in the sections that follow.

The network configuration for the model case prior to IPv6 deployment is shown in Figure 2.6.1.1. In addition, information on basic components for the model case is given in Table 2.6.1.1, and a directory of address designs is given in Table 2.6.1.2

Figure 2.6.1.1: Network Configuration for Model Case Prior to IPv6 Deployment

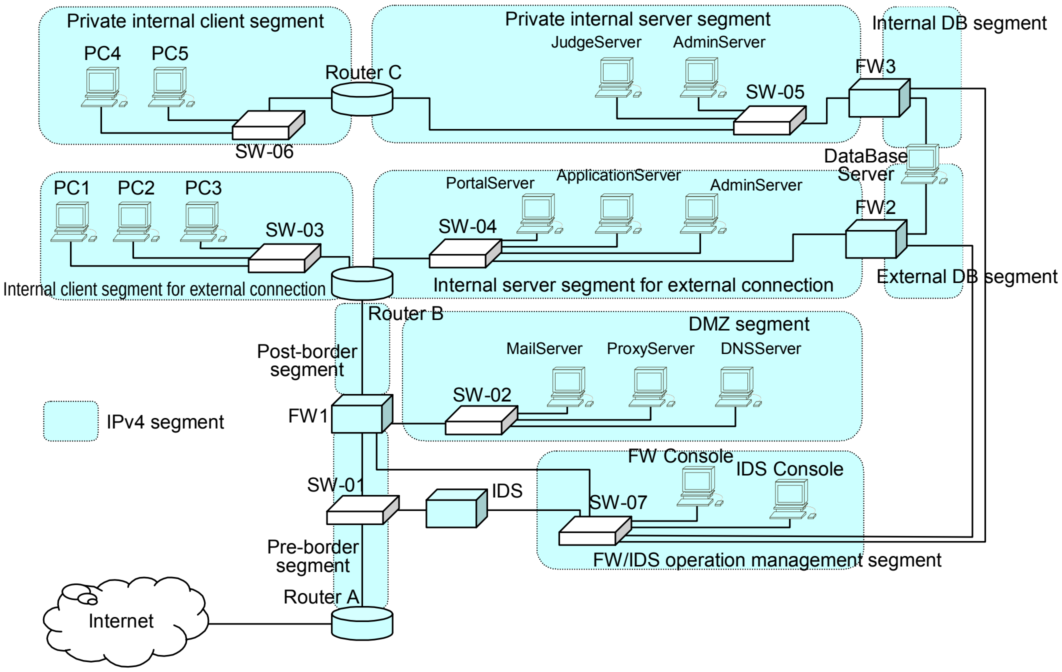


Table 2.6.1.1: Basic Components of Model Case

No.	Host Name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	RouterA	GR2000-2B	Version 07-04 OS6Bsec	eth2/0	(ISP)	(ONU)	FastEther	
				eth2/1	SW-01	eth1	FastEther	
2	RouterB	GS4000-80E1	Version 08-02-/A OS-SWE	eth0/0	FW1	eth3	FastEther	
				eth0/1	SW-03	eth1	FastEther	
				eth0/2	SW-04	eth1	FastEther	
3	RouterC	GR2000-2B	Version 07-04 OS6Bsec	eth2/0	SW-05	eth1	FastEther	
				eth2/1	SW-06	eth1	FastEther	
4	FW1	NOKIA IP350	IPSO 3.7-BUILD026 (FW-1 NG AI)	eth1	SW-01	eth2	FastEther	
				eth2	SW-02	eth1	FastEther	
				eth3	RouterB	eth0/0	FastEther	
				eth4	SW-07	eth1	FastEther	
5	FW2	NOKIA IP350	IPSO 3.7-BUILD026 (FW-1 NG AI)	eth1	SW-04	eth2	FastEther	
				eth2	DataBaseServer	fa1	FastEther	
				eth3	SW-07	eth2	FastEther	
6	FW3	NOKIA IP350	IPSO 3.7-BUILD026 (FW-1 NG AI)	eth1	SW-05	eth2	FastEther	
				eth2	DataBaseServer	fa2	FastEther	
				eth3	SW-07	eth3	FastEther	
7	IDS	Proventia A604	Real Secure7.0	eth1	SW-01	eth3	FastEther	
				eth2	SW-07	eth4	FastEther	
8	MailServer	HA8000/130A8	FreeBSD 4.9release	fa1	SW-02	eth2	FastEther	
9	ProxyServer	HA8000/130A8	Windows Server 2003 Enterprise Edition	fa1	SW-02	eth3	FastEther	
10	DNSServer	FLORA270W	RedHat Linux release9	fa1	SW-02	eth4	FastEther	
11	PotalServer	HA8000/130A8	Windows Server 2003 Enterprise Edition	fa1	SW-04	eth3	FastEther	
12	ApplicationServer	HA8000/130A8	Windows 2000 Server	fa1	SW-04	eth4	FastEther	
13	JudgeServer	HA8000/130A8	Windows 2000 Server	fa1	SW-05	eth3	FastEther	
14	DataBaseServer	HA8000/130A8	Windows 2000 Server	fa1	FW2	eth2	FastEther	
				fa2	FW3	eth2	FastEther	
15	AdminServer	HA8000/130A8	Windows 2000 Server	fa1	SW-04	eth5	FastEther	
				fa2	SW-05	eth4	FastEther	
16	FW Console	FLORA270W	Windows XP	fa			FastEther	
17	IDS Console	FLORA270W	Windows XP	fa			FastEther	
18	PC1	FLORA270W	Windows XP	fa	SW-03	eth2	FastEther	
19	PC2	FLORA270W	Windows XP	fa	SW-03	eth3	FastEther	
20	PC3	FLORA270W	Windows XP	fa	SW-03	eth4	FastEther	
21	PC4	FLORA270W	Windows XP	fa	SW-06	eth2	FastEther	
22	PC5	FLORA270W	Windows XP	fa	SW-06	eth3	FastEther	
23	SW-01	FH708TP		eth1	RouterA	eth2/1	FastEther	
				eth2	FW1	eth1	FastEther	
				eth3	IDS	eth1	FastEther	
24	SW-02	FS808TP V1		eth1	FW1	eth2	FastEther	
				eth2	MailServer	fa1	FastEther	
				eth3	ProxyServer	fa1	FastEther	
				eth4	DNSServer	fa1	FastEther	
25	SW-03	FS808TP V1		eth1	RouterB	eth0/1	FastEther	
				eth2	PC1	fa	FastEther	
				eth3	PC2	fa	FastEther	
				eth4	PC3	fa	FastEther	
26	SW-04	FS808TP V1		eth1	RouterB	eth0/2	FastEther	
				eth2	FW2	eth1	FastEther	
				eth3	PotalServer	fa1	FastEther	
				eth4	ApplicationServer	fa1	FastEther	
				eth5	AdminServer	fa1	FastEther	
27	SW-05	FS808TP V1		eth1	RouterC	eth2/0	FastEther	
				eth2	FW3	eth1	FastEther	
				eth3	JudgeServer	fa1	FastEther	
				eth4	AdminServer	fa2	FastEther	
28	SW-06	FS808TP V1		eth1	RouterC	eth2/1	FastEther	
				eth2	PC4	fa	FastEther	
				eth3	PC5	fa	FastEther	
29	SW-07	FS808TP V1		eth1	FW1	eth4	FastEther	
				eth2	FW2	eth3	FastEther	
				eth3	FW3	eth3	FastEther	
				eth4	IDS	eth2	FastEther	
				eth5	FW Console	fa	FastEther	
				eth6	IDS Console	fa	FastEther	

Table 2.6.1.2: Address Designs for Model Case Prior to IPv6 Deployment

Super Segment	Segment	Network		Address		Source		
		IPv4	IPv6	IPv4	IPv6	Host/Router	Phy. Port	Log. Port
Local gov't network	External connection segment	192.0.2.0/30		192.0.2.2		RouterA	eth2/0	eth2/0
192.0.2.0/27	Pre-border segment	192.0.2.8/29		192.0.2.9		RouterA	eth2/1	eth2/1
				192.0.2.10		FW1	eth1	eth1
	DMZ segment	192.0.2.16/29		192.0.2.17		FW1	eth2	eth2
				192.0.2.18		MailServer	fa1	fa1
				192.0.2.19		ProxyServer	fa1	fa1
				192.0.2.20		DNSserver	fa1	fa1
	Post-border segment	10.1.100.0/24		10.1.100.1		FW1	eth3	eth3
				10.1.100.2		RouterB	eth0/0	eth0/0
	Internal client segment for external connection	10.1.110.0/24		10.1.110.1		RouterB	eth0/1	eth0/1
				10.1.110.101		PC1	fa	fa
				10.1.110.102		PC2	fa	fa
				10.1.110.201		PC3	fa	fa
	Internal server segment for external connection	10.1.120.0/24		10.1.120.1		RouterB	eth0/2	eth0/2
				10.1.120.2		FW2	eth1	eth1
				10.1.120.100		AdminServer	fa1	fa1
				10.1.120.101		PortalServer	fa1	fa1
				10.1.120.102		ApplicationServer	fa1	fa1
	External database segment	10.1.130.0/24		10.1.130.1		FW2	eth2	eth2
				10.1.130.2		DataBaseServer	fa1	fa1
	Internal database segment	10.1.230.0/24		10.1.230.1		DataBaseServer	fa2	fa2
				10.1.230.2		FW3	eth1	eth1
	Privae internal server segment	10.1.220.0/24		10.1.220.1		FW3	eth2	eth2
				10.1.220.2		RouterC	eth2/0	eth2/0
				10.1.220.100		AdminServer	fa2	fa2
				10.1.220.101		JudgeServer	fa1	fa1
	Private internal client segment	10.1.210.0/24		10.1.210.1		RouterC	eth2/1	eth2/1
				10.1.210.101		PC4	fa	fa
				10.1.210.102		PC5	fa	fa
	FW/IDS operation management segment	10.1.500.0/24		10.1.500.1		FW1	eth4	eth4
				10.1.500.2		FW2	eth3	eth3
				10.1.500.3		FW3	eth3	eth3
				10.1.500.4		IDS	fa	fa
				10.1.500.11		FW Console	fa	fa
				10.1.500.12		IDS Console	fa	fa

2.6.2 Case of IPv6 Deployment Using Tunnel Method

Configuration Overview

An overview of a configuration for a local government network using the tunnel method of IPv6 deployment is shown in Figure 2.6.2.1.

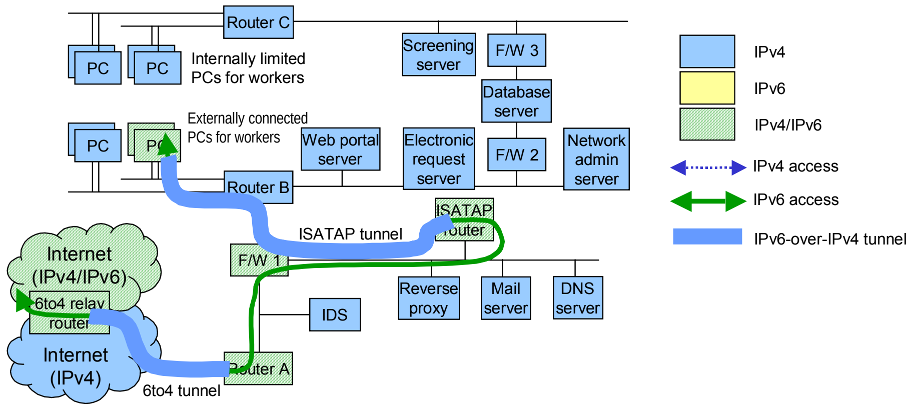


Figure 2.6.2.1: Configuration Overview of IPv6 Deployment Using Tunnel Method

The tunnel method enables IPv6 packets to transfer temporarily through a mainly IPv4-based network environment by maximizing the use of the IPv6-over-IPv4 tunneling function that encapsulates IPv6 packets into IPv4 packets. By changing just some of the devices on a local government network to IPv6, it is possible to migrate specific terminals or network segments to IPv6.

In Figure 2.6.2.1, two types of IPv6-over-IPv4 tunnels, 6to4 and ISATAP, are used in particular, and provide one example of how IPv6 can be introduced. The features of this configuration are given below:

- 6to4 is used for the tunnel that connects to the Internet, because it can easily make IPv6 connections. (If it is important to assure quality of service, the fixed tunnel service already provided by some ISPs should be used.)
- On local government networks, in order to maintain strict security management, since internal information of items like tunnel packets (protocol No. 41) cannot be checked at firewalls, in principle these items are not passed.
- For their internal LAN, we are assuming that most local government networks use private addresses. Thus, the backbone network portion of the

internal LAN is kept at IPv4, and any IPv6-compliant terminals use the ISATAP tunnel to make IPv6 connections.

- Both 6to4 and ISATAP are implemented on a practical level in main OSs, and are highly useful tunnel protocols.

6to4 uses 6to4 relay routers that are generally available on the Internet through large ISPs and other sources, and a tunnel is formed between a 6to4 relay router and Router A (external connection router) of the local government network. Here, Router A can use a fixed IPv4 global address to generate a unique IPv6 address (prefix) of /48, and it can then use this address to design IPv6 addresses for the network under it. (Figure 2.6.2.2)

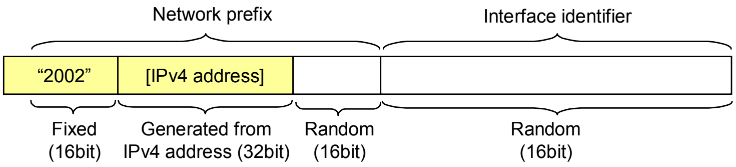


Figure 2.6.2.2: IPv6 Address in a 6to4 Tunnel

The following URL can be referred to for publically available information on 6to4 relay routers.

http://www.6to4.jp/relay-list.html

If 6to4 is used in this way, basically, IPv6 can be tentatively introduced without concluding an IPv6 contract with an ISP. However, the following constraints need to be considered:

- Since 6to4 relay router service is not a commercial service, it should be made a tentative measure for conducting IPv6 trials.
- If the IPv6 network scale is expanded while the 6to4 tunnel is being used, caution must be taken at the time an IPv6 line contract is concluded with an ISP after this, as large-scale address renumbering will occur at this time.
- If a 6to4 tunnel is to be placed, caution must be taken in its use, as there are cases in which the outgoing and incoming paths are different if communication in principle takes place between two points. (Since multiple numbers of 6to4 relay routers exist throughout the world, it is possible that a return path will pass through a different 6to4 relay router than was specified for the outgoing path.)

A big feature of ISATAP is that this tunnel can be applied in networks designed with IPv4 private addresses. In Figure 2.6.2.1, an ISATAP router has been installed in the DMZ and an ISATAP tunnel can be placed between any IPv6-compliant terminals on the internal LAN. Conversely, restrictions for communications using the ISATAP tunnel can be managed by setting tunnel packet (protocol No. 41) access restrictions in the firewall or Router B (backbone router).

Even in an internal LAN where IPv4 private addresses have been used to divide the network into multiple segments, an ISATAP tunnel can be used to build one virtual IPv6 segment that uses the ISATAP router as the default router. The ISATAP router advertises at the RA on the ISATAP terminal the network prefix that was allotted from the IPv6 network side, and the ISATAP terminal, in adherence to ISATAP address generation rules, can use the network prefix that was advertised on the RA and the IPv4 address to generate an IPv6 address. (Figure 2.6.2.3)

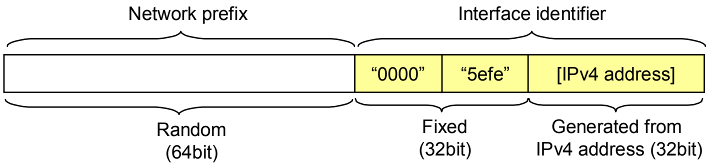


Figure 2.6.2.3: IPv6 Address in an ISATAP Tunnel

If an ISATAP tunnel is used, the ISATAP terminal can automatically recognize the ISATAP router by registering the record of the ISATAP router that the ISATAP terminal refers to. This enables a dramatic reduction in the number of setting procedures that are made on the terminal side.

Since many other methods of realizing IPv6 reachability are possible using not only the configuration shown here but also other tunneling technologies, flexible consideration needs to be given in response to network environmental conditions and other required conditions.

Due to the features of the tunnel method in realizing IPv6 connectivity by applying IPv6-over-IPv4 tunneling in segments that do not support IPv4, the IPv6 deployment patterns being assumed are mainly of the staged replacement type. Every effort should be made to avoid the tunnel method in deployment patterns of the independent merging type where we recommend configuring a native (dual stack) IPv6 system that is simple and takes maximum advantage of the merits of IPv6.

Example of Tunnel Method Application in the Model Case

Figure 2.6.2.4 shows a concrete network configuration where the overview configuration shown in Figure 2.6.2.1 is applied to the model case. In addition, a directory of address designs supporting this network configuration is given in Table 2.6.2.1. For information on basic components, see Table 2.6.1.1 (above).

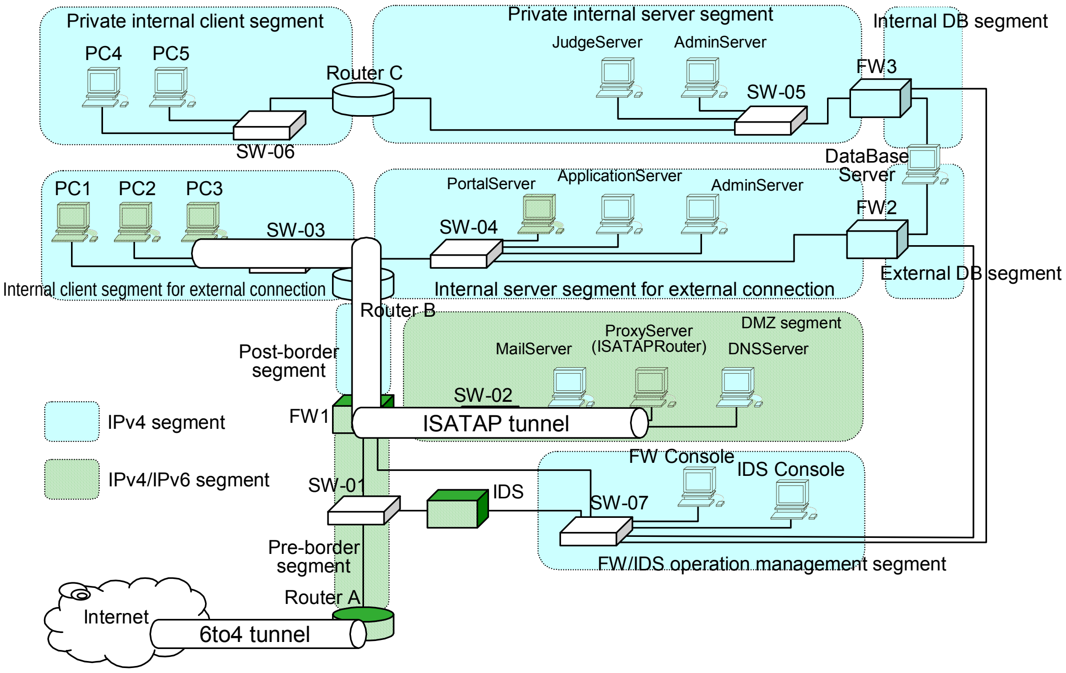


Figure 2.6.2.4: IPv6 Deployment Network Configuration for Model Case Using Tunnel Method

In the network configuration shown in Figure 2.6.2.4, the external connection router (Router A) and the firewall at the borders of the network have been made to comply with IPv6 first. The ISATAP router makes this possible using the ISATAP router functions of the existing ProxyServer OS (Windows Server 2003). By adding a record consisting of "ISATAP IN CNAME ProxyServer" to the DNS server at this time, the ISATAP terminal will be able to automatically recognize the ISATAP router. All effort should be made to use an IPv6-compliant IDS.

The important point in the model case prior to IPv6 deployment is to migrate only the minimum possible network devices to IPv6. Form the point of security management, we stressed the importance of having the firewall be IPv6 compliant, but the high-cost, large-scale router/L3 switch (Router B) is being left as is.

Table 2.6.2.1: Address Designs for IPv6 Deployment Network Configuration Using Tunnel Method

Super Segment	Segment	Network		Address		Source		
		IPv4	IPv6	IPv4	IPv6	Host/Router	Phy. Port	Log. Port
Local gov/t network 192.0.2.0/27	External connection segment	192.0.2.0/30		192.0.2.2		RouterA	eth2/0	eth2/0
	Pre-border segment	192.0.2.8/29	2002:c000:0202:10::/64	192.0.2.9	2002:c000:0202:10::1	RouterA	eth2/1	eth2/1
				192.0.2.10	2002:c000:0202:10::2	FW1	eth1	eth1
	DMZ segment	192.0.2.16/29	2002:c000:0202:100::/64	192.0.2.17	2002:c000:0202:50::1	FW1	eth2	eth2
				192.0.2.18	2002:c000:0202:50::18	MailServer	fa1	fa1
				192.0.2.19	2002:c000:0202:50::19	ProxyServer	fa1	fa1
				192.0.2.20	2002:c000:0202:50::20	DNSserver	fa1	fa1
					2002:c000:0202:100:0:5efe:192.0.2.227	ISATAPRouter	-	if2
	Post-border segment	10.1.100.0/24		10.1.100.1		FW1	eth3	eth3
				10.1.100.2		RouterB	eth0/0	eth0/0
	Internal client segment for external connection	10.1.110.0/24	2002:c000:0202:100::/64	10.1.110.1		RouterB	eth0/1	eth0/1
				10.1.110.101		PC1	fa	fa
					2002:c000:0202:100:0:5efe:10.1.110.101	PC1	-	tunnel
				10.1.110.102		PC2	fa	fa
					2002:c000:0202:100:0:5efe:10.1.110.102	PC2	-	tunnel
				10.1.110.201		PC3	fa	fa
					2002:c000:0202:100:0:5efe:10.1.110.201	PC3	-	tunnel
	Internal server segment for external connection	10.1.120.0/24	2002:c000:0202:100::/64	10.1.120.1		RouterB	eth0/2	eth0/2
				10.1.120.2		FW2	eth1	eth1
				10.1.120.100		AdminServer	fa1	fa1
				10.1.120.101		PortalServer	fa1	fa1
					2002:c000:0202:100:0:5efe:10.1.120.101	PortalServer	-	tunnel
				10.1.120.102		ApplicationServer	fa1	fa1
	External database segment	10.1.130.0/24	-	10.1.130.1		FW2	eth2	eth2
				10.1.130.2		DataBaseServer	fa1	fa1
	Internal database segment	10.1.230.0/24	-	10.1.230.1		DataBaseServer	fa2	fa2
				10.1.230.2		FW3	eth1	eth1
	Private internal server segment	10.1.220.0/24	-	10.1.220.1		FW3	eth2	eth2
				10.1.220.2		RouterC	eth2/0	eth2/0
				10.1.220.100		AdminServer	fa2	fa2
				10.1.220.101		JudgeServer	fa1	fa1
	Private internal client segment	10.1.210.0/24	-	10.1.210.1		RouterC	eth2/1	eth2/1
				10.1.210.101		PC4	fa	fa
				10.1.210.102		PC5	fa	fa
	FW/IDS operation management segment	10.1.500.0/24		10.1.500.1		FW1	eth4	eth4
				10.1.500.2		FW2	eth3	eth3
				10.1.500.3		FW3	eth3	eth3
				10.1.500.4		IDS	fa	fa
				10.1.500.11		FW Console	fa	fa
				10.1.500.12		IDS Console	fa	fa

Points of Caution in the Tunneling Method

There is a variety of local government network configurations, and since recent IPv6-compliant equipment supports a large number of tunnel protocols, a large number of tunnel configuration variations is possible. Below we provide some points concerning minimum considerations that should be addressed in designing and building a tunnel to suit each of the environmental conditions.

(1) Filtering in firewalls and routers

We believe that at the present time, there are no firewalls that are equipped with filtering functions supporting IPv6-over-IPv4 tunnel packets, i.e. that are capable of checking the content of encapsulated IPv6 packets. Firewalls thus can only be set to either allow all tunnel packets (protocol No. 41) to pass or to block them. Considering the need for security on local government networks, it is dangerous to allow tunnel packets to pass unconditionally at the borders of the network. If the packets are allowed to pass, sufficient consideration must be given to the impact on security.

Some normal routers, however, are equipped with filtering settings that can block tunnel packets from the beginning without being aware of them. If this type of router is present in the tunnel segment, even if tunnel settings have been made, caution must be given to the possibility that the tunnel may not be created as expected.

(2) Tunnel configuration patterns

Possible candidates for 6to4 and ISATAP tunnel termination points are shown in Figure 2.6.2.5.

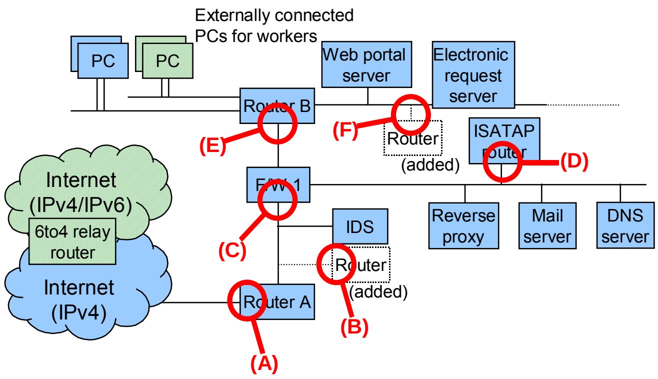


Figure 2.6.2.5: Possible Candidates for 6to4 and ISATAP Termination Points

First, in creating a 6to4 tunnel, if the installation location for the 6to4 tunnel terminator that is to terminate the tunnel in opposition to the publicly available 6to4 relay router is a location that has an IPv4 global address, basically, it is possible to terminate 6to4. When considering "Filtering in firewalls and routers," however, locations (A) to (C) in Figure 2.6.2.5 are realistic candidates for installation locations. Location (A) is a place where a terminator can be installed relatively easily by replacing Router A (external connection router) or upgrading the software, and the example in Figure 2.6.2.1 is one in which (A) was selected. If it is difficult for Router A to support 6to4, locations (B) and (C) are possible alternatives. Though (B) requires a new, 6to4-compliant router, if processing power is not a concern, this offers a relatively low-cost solution. Location (C) is possible if the firewall supports 6to4, but in addition to the original functions of the firewall, sufficient consideration must be given to processing power in the event that 6to4 termination is to be performed.

Next, in creating an ISATAP tunnel, locations (D) to (F) in Figure 2.6.2.5 are considered candidates for locations where an ISATAP router could be installed. Basically, an ISATAP router should be installed at the border between the IPv6 network and the IPv4 (private) network. Accordingly, location (D), which is the DMZ shown in Figure 2.6.2.1, is considered to be the most natural place for an ISATAP router to be installed. Location (E) needs as much consideration as (C) does in the case of 6to4. Concerning (F), as long as Router B (backbone router, L3 switch) is not made to be IPv6-compliant, an ISATAP router cannot be installed here, because an IPv6 prefix cannot be drawn to the section where (F) is located.

(3) Compatibility with applications

In using dynamic tunnels such as 6to4, ISATAP, or Teredo, these tunnels can be terminated as is at the user's terminal, and since it is also relatively easy to make settings in the user's terminal so that it can dynamically create a tunnel, IPv6 connections are easily made. Caution is required, however, as some IPv6-compliant applications are not able to recognize virtual IPv6 interfaces generated in these dynamic tunnels.

Below are some examples of IPv6 interfaces in Windows XP, and in these cases, Interfaces 2, 3, and 5 are not recognized by some applications.

```
Interface 5: Teredo Tunneling Pseudo-Interface (Virtual interface)
Interface 4: Ethernet: Local area connection (Real interface)
Interface 3: 6to4 Tunneling Pseudo-Interface (Virtual interface)
Interface 2: Automatic Tunneling Pseudo-Interface (Virtual
interface)
Interface 1: Loopback Pseudo- Interface
```

(4) MTU (Maximum Transmission Unit)

Since tunnel packets normally encapsulate IPv6 packets in IPv4 packets, the length of all packets is uniformly as much as 20 bytes longer. Accordingly, if a large path MTU is set for real IPv6 network segments in particular, it is possible for the MTU to be exceeded in IPv4 network segments that generate tunnels. Caution is advised, since problems such as lower transmission speeds due to the fragmentation of packets, the loss of packets, or communication failures can occur as a result.

Possible countermeasures are as follows:

- To ensure that Path MTU Discovery[3] is functioning normally, check the firewall or router filter settings so that the ICMPv6 message (Packet Too Big) is not blocked.
- Set the Path MTU for the IPv6 packet transfer portion that is not a IPv6-over-IPv4 tunnel segment to a value that is 20 bytes (the IPv4 header size) smaller than the Path MTU for the IPv4 portion of the IPv6-over-IPv4 segment[4]

(5) QoS control

Normal communications equipment cannot analyze the content of packet data that has been encapsulated into an IPv6-over-IPv4 tunnel packet. As a result, when data of a variety of types and characteristics, such as file data or sound/moving picture data, is transferred through a tunnel path, priority control over this data is no longer possible especially when communications equipment causing a bottleneck is present in the tunnel segment. Thus, if control over communications quality for each service is required, continued use of the tunnel method should be avoided.

In cases like this configuration where a tunnel is not used at the border area, it is possible to establish QoS control settings in the segment interface at the stage just prior to the border of Router A, for example.

(6) Band and overhead

The following two points of caution concerning transfer capability must be considered when using an IPv6-over-IPv4 tunnel:

- The larger header caused by encapsulation
- The larger transfer load and the occurrence of delays caused by capsule processing

[3] In IPv6, the occurrence of fragmentation is prohibited on the communications path, and it is equipped with a Path MTU Discovery function that detects in advance the smallest value of all node equipment on the communications path at the time communication starts.

[4] RFC2460 stipulates that the minimum MTU size in IPv6 must be at least 1280 bytes.

Concerning the first point, since packet length increases by as much as 20 bytes uniformly for each packet, this impacts packet transfer capabilities for all IPv4 transfer devices in the tunnel segments. The second point concerns processing related to the encapsulation and decapsulation of tunnel packets, and in principle, tunnel processing capabilities for devices terminating both ends of the tunnel are impacted. Even when tunnel methods are used as a tentative measure, it is important to configure and management a network that recognizes whether or not a bottleneck exists and where.

2.6.3 Case of IPv6 Deployment Using Translator Method

Configuration Overview

An overview of a configuration for a local government network using the translator method of IPv6 deployment is shown in Figure 2.6.3.1.

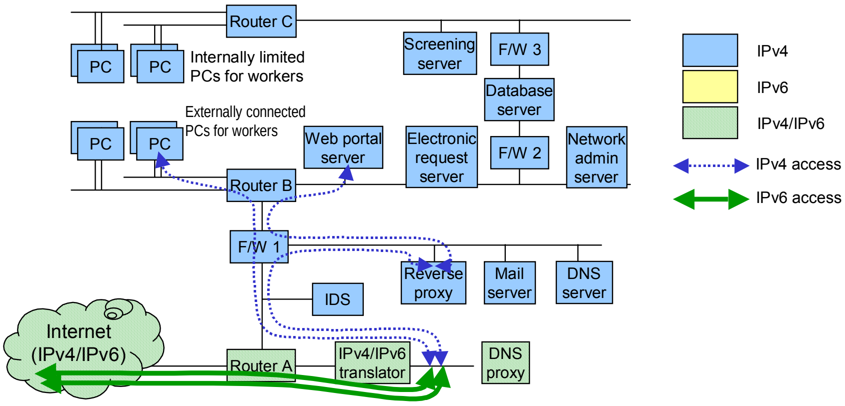


Figure 2.6.3.1: Configuration Overview of IPv6 Deployment using Translator Method

This method of IPv6 deployment achieves virtual IPv6 support in mainly IPv4 network environments by introducing a translator possessing IPv4/IPv6 protocol conversion functions around the external interface of the local government network. As shown in Figure 2.6.3.1, the translator can be installed from Router A, or interpositioned between Router A and the firewall. From the perspective of minimizing impact on the existing network, considering that the risk of pushing new equipment between Router A and the firewall is large, in this configuration, the choice was made to install the translator from Router A. Though the translator could also be installed in the DMZ, this option will not be discussed here, as it is similar to the configuration in section 2.6.4, "Case of IPv6 Deployment Using Proxy Method," coming next.

Figure 2.6.3.1 assumes a NAT-PT translator, and a DNS proxy that supports this translator is also provided. The DNS proxy is linked to the existing DNS server and the translator, and in the domain name's name resolution requested by any resolver, IPv4/IPv6 protocol translation is automatically achieved when a response with a virtual IP address is given.

Due to the features of the translator method that allow all efforts to maintain the existing IPv4 system as is and that converts all IPv4/IPv6 protocols, the IPv6 deployment patterns being assumed are mainly of the staged replacement type.

Example of Translator Method Application in the Model Case

Figure 2.6.3.2 shows a concrete network configuration where the overview configuration shown in Figure 2.1.3.1 is applied to the model case. In addition, information on basic components supporting this network configuration is given in Table 2.6.3.1, and a directory of address designs is given in Table 2.6.3.2.

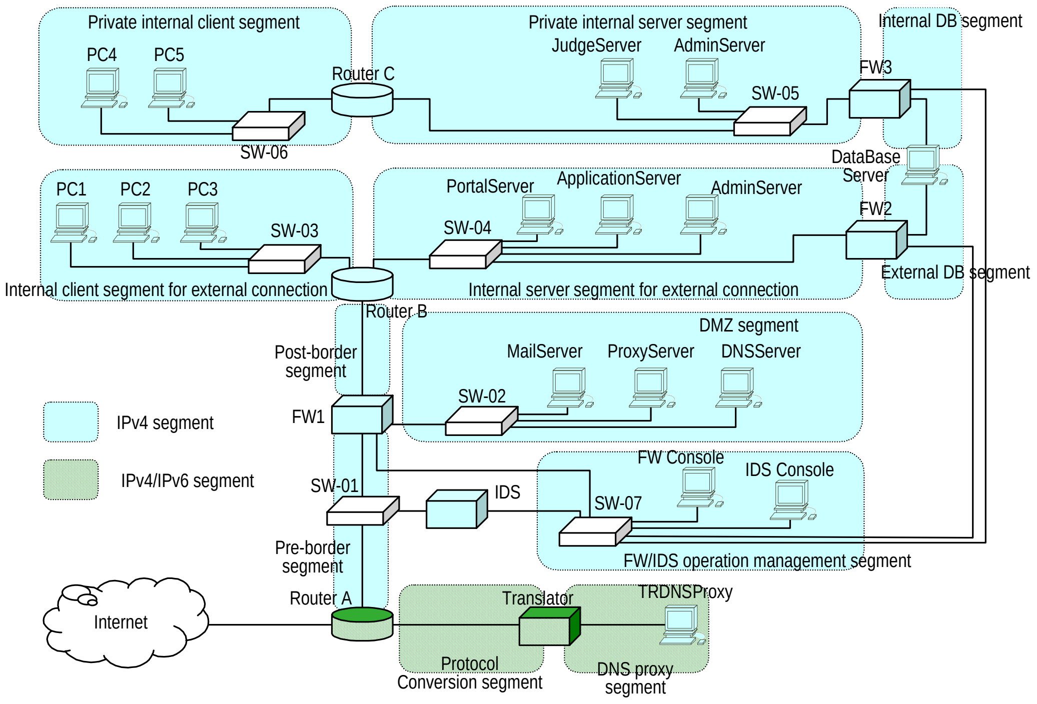


Figure 2.6.3.2: IPv6 Deployment Network Configuration for Model Case Using Translator Method

In the network configuration shown in Figure 2.6.3.2, the external connection router (Router A) alone has been made to comply with IPv6 first, then a translator and a DNS proxy for the translator were newly installed. In addition, a portion of the registrations and settings for the DNS server was changed. No basic changes for any other network devices are required.

Table 2.6.3.1: Basic Components of Model Case

No.	Host Name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	RouterA	GR2000-2B	Version 07-04 OS6Bsec	eth2/0	(ISP)	(ONU)	FastEther	
				eth2/1	SW-01	eth1	FastEther	
				eth2/2	Translator	eth1	FastEther	
2	RouterB	GS4000-80E1	Version 08-02-/A OS-SWE	eth0/0	FW1	eth3	FastEther	
				eth0/1	SW-03	eth1	FastEther	
				eth0/2	SW-04	eth1	FastEther	
3	RouterC	GR2000-2B	Version 07-04 OS6Bsec	eth2/0	SW-05	eth1	FastEther	
				eth2/1	SW-06	eth1	FastEther	
4	FW1	NOKIA IP350	IPSO 3.7-BUILD026 (FW-1 NG AI)	eth1	SW-01	eth2	FastEther	
				eth2	SW-02	eth1	FastEther	
				eth3	RouterB	eth0/0	FastEther	
				eth4	SW-07	eth1	FastEther	
5	FW2	NOKIA IP350	IPSO 3.7-BUILD026 (FW-1 NG AI)	eth1	SW-04	eth2	FastEther	
				eth2	DataBaseServer	fa1	FastEther	
				eth3	SW-07	eth2	FastEther	
6	FW3	NOKIA IP350	IPSO 3.7-BUILD026 (FW-1 NG AI)	eth1	SW-05	eth2	FastEther	
				eth2	DataBaseServer	fa2	FastEther	
				eth3	SW-07	eth3	FastEther	
7	IDS	Proventia A604	Real Secure7.0	eth1	SW-01	eth3	FastEther	
				eth2	SW-07	eth4	FastEther	
8	Translator	AG8100S-T	AG OS rev.3.4.14	eth1	RouterA	eth2/2	FastEther	
				eth2	TRDNSProxy	eth0	FastEther	
9	TRDNSProxy	HA8000/110D8	RedHat Linux release9	eth0	Translator	eth2	FastEther	
10	MailServer	HA8000/130A8	FreeBSD 4.9release	fa1	SW-02	eth2	FastEther	
11	ProxyServer	HA8000/130A8	Windows Server 2003 Enterprise Edition	fa1	SW-02	eth3	FastEther	
12	DNSServer	FLORA270W	RedHat Linux release9	fa1	SW-02	eth4	FastEther	
13	PotalServer	HA8000/130A8	Windows Server 2003 Enterprise Edition	fa1	SW-04	eth3	FastEther	
14	ApplicationServer	HA8000/130A8	Windows 2000 Server	fa1	SW-04	eth4	FastEther	
15	JudgeServer	HA8000/130A8	Windows 2000 Server	fa1	SW-05	eth3	FastEther	
16	DataBaseServer	HA8000/130A8	Windows 2000 Server	fa1	FW2	eth2	FastEther	
				fa2	FW3	eth2	FastEther	
17	AdminServer	HA8000/130A8	Windows 2000 Server	fa1	SW-04	eth5	FastEther	
				fa2	SW-05	eth4	FastEther	
18	FW Console	FLORA270W	Windows XP	fa			FastEther	
19	IDS Console	FLORA270W	Windows XP	fa			FastEther	
20	PC1	FLORA270W	Windows XP	fa	SW-03	eth2	FastEther	
21	PC2	FLORA270W	Windows XP	fa	SW-03	eth3	FastEther	
22	PC3	FLORA270W	Windows XP	fa	SW-03	eth4	FastEther	
23	PC4	FLORA270W	Windows XP	fa	SW-06	eth2	FastEther	
24	PC5	FLORA270W	Windows XP	fa	SW-06	eth3	FastEther	
25	SW-01	FH708TP		eth1	RouterA	eth2/1	FastEther	
				eth2	FW1	eth1	FastEther	
				eth3	IDS	eth1	FastEther	
26	SW-02	FS808TP V1		eth1	FW1	eth2	FastEther	
				eth2	MailServer	fa1	FastEther	
				eth3	ProxyServer	fa1	FastEther	
				eth4	DNSServer	fa1	FastEther	
27	SW-03	FS808TP V1		eth1	RouterB	eth0/1	FastEther	
				eth2	PC1	fa	FastEther	
				eth3	PC2	fa	FastEther	
				eth4	PC3	fa	FastEther	
28	SW-04	FS808TP V1		eth1	RouterB	eth0/2	FastEther	
				eth2	FW2	eth1	FastEther	
				eth3	PotalServer	fa1	FastEther	
				eth4	ApplicationServer	fa1	FastEther	
				eth5	AdminServer	fa1	FastEther	
29	SW-05	FS808TP V1		eth1	RouterC	eth2/0	FastEther	
				eth2	FW3	eth1	FastEther	
				eth3	JudgeServer	fa1	FastEther	
				eth4	AdminServer	fa2	FastEther	
30	SW-06	FS808TP V1		eth1	RouterC	eth2/1	FastEther	
				eth2	PC4	fa	FastEther	
				eth3	PC5	fa	FastEther	
31	SW-07	FS808TP V1		eth1	FW1	eth4	FastEther	
				eth2	FW2	eth3	FastEther	
				eth3	FW3	eth3	FastEther	
				eth4	IDS	eth2	FastEther	
				eth5	FW Console	fa	FastEther	
				eth6	IDS Console	fa	FastEther	

Table 2.6.3.2: Address Designs for IPv6 Deployment Network Configuration Using Translator Method

Super Segment	Segment	Network		Address		Source		
		IPv4	IPv6	IPv4	IPv6	Host/Router	Phy. Port	Log. Port
Local gov't network 192.0.2.0/27 2001:db8:1000::/48	External connection segment	192.0.2.0/30	2001:db8::/64	192.0.2.2	2001:db8::2	RouterA	2/0	2/0
	Protocol conversion segment	192.0.2.24/30	2001:db8:1000:20::/64	192.0.2.25	2001:db8:1000:20::1	RouterA	2/2	2/2
				192.0.2.26	2001:db8:1000:20::2	Translator	eth1	eth1
	DNS proxy segment	192.0.2.28/30	2001:db8:1000:30::/64	192.0.2.29	2001:db8:1000:30::1	Translator	eth2	eth2
				192.0.2.30	2001:db8:1000:30::2	TRDNSProxy	fa	fa
	Pre-border segment	192.0.2.8/29		192.0.2.9		RouterA	2/3	2/3
				192.0.2.10		FW1	eth1	eth1
	DMZ segment	192.0.2.16/29		192.0.2.17		FW1	eth2	eth2
				192.0.2.18		MailServer	fa1	fa1
				192.0.2.19		ProxyServer	fa1	fa1
				192.0.2.20		DNSserver	fa1	fa1
	Post-border segment	10.1.100.0/24		10.1.100.1		FW1	eth3	eth3
				10.1.100.2		RouterB	eth0/0	eth0/0
	Internal client segment for external connection	10.1.110.0/24		10.1.110.1		RouterB	eth0/1	eth0/1
				10.1.110.101		PC1	fa	fa
				10.1.110.102		PC2	fa	fa
				10.1.110.201		PC3	fa	fa
	Internal server segment for external connection	10.1.120.0/24		10.1.120.1		RouterB	eth0/2	eth0/2
				10.1.120.2		FW2	eth1	eth1
				10.1.120.100		AdminServer	fa1	fa1
				10.1.120.101		PortalServer	fa1	fa1
				10.1.120.102		ApplicationServer	fa1	fa1
	External database segment	10.1.130.0/24		10.1.130.1		FW2	eth2	eth2
				10.1.130.2		DataBaseServer	fa1	fa1
	Internal database segment	10.1.230.0/24		10.1.230.1		DataBaseServer	fa2	fa2
				10.1.230.2		FW3	eth1	eth1
	Private internal server segment	10.1.220.0/24		10.1.220.1		FW3	eth2	eth2
				10.1.220.2		RouterC	eth2/0	eth2/0
				10.1.220.100		AdminServer	fa2	fa2
				10.1.220.101		JudgeServer	fa1	fa1
	Private internal client segment	10.1.210.0/24		10.1.210.1		RouterC	eth2/1	eth2/1
				10.1.210.101		PC4	fa	fa
				10.1.210.102		PC5	fa	fa
	FW/IDS operation management segment	10.1.500.0/24		10.1.500.1		FW1	eth4	eth4
				10.1.500.2		FW2	eth3	eth3
				10.1.500.3		FW3	eth3	eth3
				10.1.500.4		IDS	fa	fa
				10.1.500.11		FW Console	fa	fa
				10.1.500.12		IDS Console	fa	fa

Points of Caution in the Translator Method

Here we provide some points concerning minimum considerations that should be addressed in performing IPv6 deployment using translators. These points are based on examples of network construction utilizing IPv4/IPv6 translators in local government networks.

(1) Locations for installing translators

Two types of locations for installing translators are as follows:

- Push type
- Place type

The Push type involves inserting a translator between two devices that are directly connected to each other, and the Place type involves leaving the original device configuration as is and adding a new network segment to which the translator is connected. The intuitive image of converting protocols often assumes the Push type, but from the perspective of migrating the existing network to IPv6 while continuing services, the Place type has less impact on the existing network.

Below, we summarize the advantages and disadvantages of the Place type compared with the Push type:

< Advantages >

- Communication packets that do not require translation can be transferred along the usual path independently of the translator.
- Along with the above advantage, even if the translator that was introduced is of a lower level than the network processing capacity of the existing network, it does not impact the existing network.

< Disadvantages >

- Efficiency is poor, since packets requiring translation must pass twice through the router where the translator is placed.
- If the router where the translator is placed does not have extra ports, additional ports will be necessary.

Considering the above, in the initial stage of IPv6 migration, the Place type of translator installation is easier due to the lower risk.

(2) Linking with the DNS proxy

The introduction of a DNS proxy is indispensable for realizing automatic protocol conversion utilizing name resolution of the domain name. The following two DNS server functions are required:

(a) When an external network terminal accesses a server or other device on a local government's internal network

To realize automatic IPv4/IPv6 protocol translation, a DNS proxy must be designated as a master DNS server with the local government network as its zone. At this time, this DNS proxy accepts non-recursive DNS inquiries. (Content mode)

(b) When a server or other device on a local government's internal network accesses an external network terminal

To realize automatic IPv4/IPv6 protocol translation, a DNS proxy must be designated as the default DNS server of local government internal terminals. At this time, this DNS proxy accepts recursive DNS inquiries. (Cache mode)

In realizing the two types of access described above, a number of points of caution are given below.

Concerning type (a), "When an external network terminal accesses a server or other device on a local government's internal network," there are cases when it is not absolutely necessary to use DNS proxy functions. In most cases, there are not so many types of servers (legacy servers whose domain names are registered in the DNS) on the local government network that are accessible from the outside. Accordingly, rather than setting a mechanism that activates the DNS proxy and generates a virtual address for each query it receives requiring translation, the methods given below achieve simple translation without the use of a DNS proxy.

- Statically register virtual IPv6 addresses in advance in the translator's conversion entry for each real IPv4 address of the servers on the local government's internal network.
- Then, add these virtual IPv6 addresses to the existing DNS server registration as AAAA records.

The above two settings simplify the management of virtual addresses, allowing translation to occur without changing registrations to the ISP of the master DNS server that makes the local government network a zone.

For example, if IPv6-to-IPv4 protocol conversion is to be performed for a communication sent to a proxy server in the network in Figure 2.6.3.2, as shown in Table 2.6.3.3, a virtual IPv6 address for the proxy server is statically registered for the real IPv4 address in the conversion entry of the translator.

Table 2.6.3.3: Positioning a Virtual IPv6 Address for a Real IPv4 Address

Host name	Real IPv4 Address	Virtual IPv6 Address
ProxyServer	192.0.2.19 /29	2001:db8:1000:21::1 /64

In addition, if the following is also registered in the DNS server, IPv6-to-IPv4 protocol conversion in the reverse proxy will be possible.

```
ProxyServer          IN         AAAA    2001:db8:1000:21::1
```

Concerning type (b), "When a server or other device on a local government's internal network accesses an external network terminal," in the network settings of the local government's internal terminals, it is necessary to designate a DNS proxy as a default proxy. Caution is necessary, since this often causes unexpected operations to occur. In other words, a terminal supporting IPv4/IPv6 dual stack accesses an IPv4 server, for example. If a dual stack terminal first asks that an IPv6-based (AAAA record) name be resolved[5], the name resolution would fail if the DNS server is a normal one, and immediately after that, an IPv4-based (A record) name would be successfully resolved, enabling IPv4 native communication to start. If a DNS proxy is used, however, even if IPv6-based name resolution fails, the DNS proxy itself would automatically (on its own) make the IPv4-based name resolution succeed, and the virtual IPv6 address supporting that IPv4 address would be given in reply to the dual stack terminal (resolver). As a result, even in cases where simple IPv4 native access is possible, IPv4/IPv6 translation is forced, and sometimes this causes problems such as deterioration of response or a loss of packets. The function of this sort of DNS proxy is native access, in other words, to prevent natural communications between IPv4 terminals or between IPv6 terminals, and protocol conversion can become the cause of unexpected problems. Accordingly, if the DNS proxy is to be designated as a fixed default DNS, sufficient study needs to be conducted beforehand. As a realistic measure, the need for IPv4/IPv6 translation described in type (b), "When a server or other device on a local government's internal network accesses an external network terminal" should be reconsidered, and if it is considered necessary, then it is probably good to designate the DNS proxy as the default DNS.

(3) Address pool for conversion

When using the translator in actual operation, it is first necessary to secure a pool of tentative IP addresses for use by the translator during protocol conversion. An image of tentative IP addresses being used via a translator is shown in Figure 2.6.2.3.

[5] In Windows XP, name resolution places priority on IPv6.

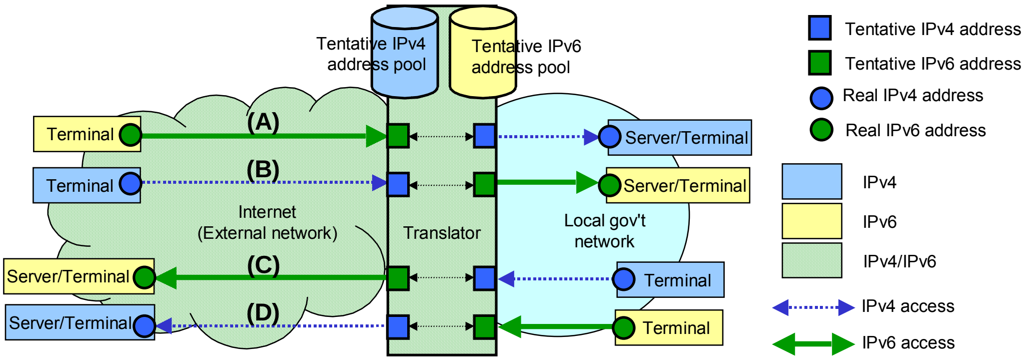


Figure 2.6.3.3: Image of Tentative IP Addresses Being Used via a Translator

Each time a session requiring protocol conversion occurs, the translator performs translation by assigning a tentative IPv4 address and a tentative IPv6 address to the real IPv6 address and the real IPv4 address, respectively. It is therefore basically necessary to secure in advance a pool of both IPv4 addresses and IPv6 addresses that can be used for several translation sessions.

When actual IPv6 deployment occurs, although it is possible for IPv6 addresses for the pool to secure sufficient address space, there will be a problem securing IPv4 addresses for the pool. While the problem can be solved by securing IPv4 addresses for a pool to be used for the local government's internal network and using them as a suitable pool of private addresses, caution is advised, since IPv4 global addresses that are limited for allotment to each local government must be secured as addresses for a pool to be used for external networks. Since it is difficult in practice to secure a sufficient number of IPv4 global addresses, it is necessary to economize on the number of addresses used by studying, for instance, the use of an IP masquerade that realizes virtually the occurrence of a number of sessions by using different port numbers with one IP address.

As described in section 2.4.2, "Translation," the usual aim in using a translator is to perform translation at locations (A) or (C) in Figure 2.4.2.1 and Figure 2.6.3.3. In these cases, compliance is possible if the IPv4 addresses for the pool are used as IPv4 private addresses for the local government's internal network.

(4) Necessity of ALG for special applications

Since NAT-PT or TRT and other translators perform protocol conversions in layer 3 or layer 4, complete translation cannot be performed in the communications of applications with IP address information that is included in the data sections of higher layers. FTP and SIP are two such applications.

Concerning FTP, many normal translators support FTP conversion and cases of problems are rare. Also, since the number of cases requiring protocol conversion during access from an FTP client to an FTP server is limited, except for some special use environments, there is probably not much need for concern.

The penetration of applications based on SIP is expected to dramatically grow in scale from now on with the spread of IPv6. A feature of SIP applications is that they are capable of realizing direct, bi-directional communications between end-to-end terminals. In local government networks originally, until ALG is introduced, we believe it is more prudent, for future considerations, to study introducing a network environment that can use IPv6-compliant SIP clients from the beginning than to study the realization of SIP communications between IPv4 clients and IPv6 clients.

Concerning ALG, if it is absolutely necessary for actual operation, it is probably best to study introducing them individually. As for applications for which the translator performs protocol conversion, since cases of unexpected problems are possible, not only with FTP or SIP, operation should be sufficiently verified in advance of introduction.

(5) MTU

As in the case of tunneling, problems concerning MTU can also occur when a translator is applied. (See "MTU (Maximum Transmission Unit).") In other words, since packet headers become as much as 20 bytes larger when IPv4 is converted to IPv6, packet loss sometimes occurs. In the case of a translator, since the MTU straddles the two different protocols of IPv4 and IPv6 and the MTU needs to be adjusted, when a problem occurs, it is more difficult to fix than in the case of a tunnel.

For example, if a problem such as a Web screen not being displayed occurs, or if it is displayed, it is displayed only incompletely, attempts to solve the problem should probably be made through tuning efforts such as adjusting MTU values on related network equipment.

2.6.4 Case of IPv6 Deployment Using Proxy Method

Configuration Overview

An overview of a configuration for a local government network using the proxy method of IPv6 deployment is shown in Figure 2.6.4.1.

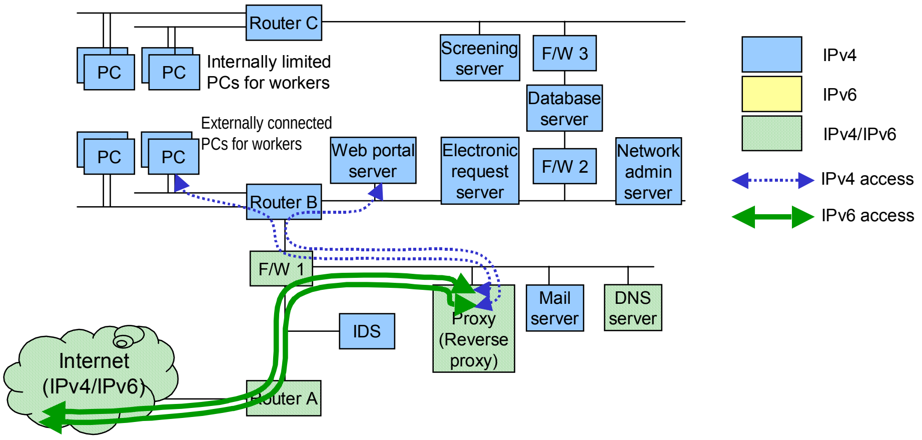


Figure 2.6.4.1: Configuration Overview of IPv6 Deployment Using Proxy Method

This method of IPv6 deployment achieves virtual IPv6 support in mainly IPv4 network environments by introducing a proxy possessing IPv4/IPv6 protocol conversion functions in the DMZ of the local government network.

Concerning the electronic request server or the Web portal server that local governments make available to the outside, the configuration that is generally adopted is one that accepts access from outside via reverse proxy. By adding an IPv4/IPv6 translation function to this reverse proxy, it is even possible for Web portal servers, electronic request servers and other devices that do not support IPv6 to accept IPv6-based accesses from the outside. At this time, AAAA records, as resource records supporting the reverse proxy, must be additionally registered in the DNS server that manages the local government zone.

PC terminals for workers on a local government network generally use Web applications and other means of external access via a normal proxy server. By adding an IPv4/IPv6 translation function to this proxy server, even PC terminals for workers that do not support IPv6 can access Web servers on external networks on an IPv6 base.

As described in section 2.4.2, "Proxy," depending on the form of use, proxy servers on a local government network function as a so-called proxy (acting as an agent of the access terminal) or a reverse proxy (acting as an agent of a public server). Figure 2.6.4.1 shows a configuration that realizes both proxy functions and reverse proxy functions in the same server.

Considering the aspect of security, the most appropriate location for installing a proxy server, like the existing proxy server, is in the DMZ. Due to the features of the proxy method that allow all efforts to maintain the existing IPv4 system as is and that converts all IPv4/IPv6 protocols, the IPv6 deployment patterns being assumed are mainly of the staged replacement type.

Example of Proxy Method Application in the Model Case

Figure 2.6.4.2 shows a concrete network configuration where the overview configuration shown in Figure 2.6.4.1 is applied to the model case. In addition, a directory of address designs supporting this network configuration is given in Table 2.6.4.1. For basic components information, see Table 2.6.1.1 (above).

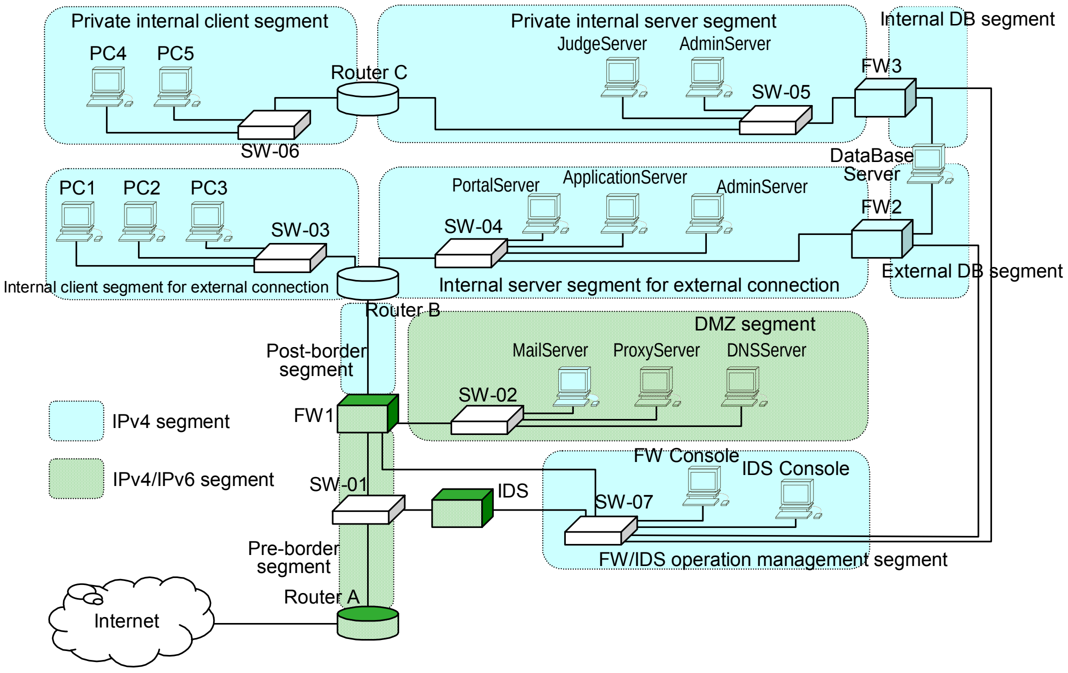


Figure 2.6.4.2: IPv6 Deployment Network Configuration for Model Case Using Proxy Method

In the network configuration shown in Figure 2.6.4.2, the external connection router (Router A) and the firewall at the borders of the network have been made to comply with IPv6 first. All effort should be made to use an IPv6-compliant IDS. ProxyServer should be made IPv6-compliant based on the Windows Server 2003, and a protocol conversion function by proxy should be realized by installing Apache-2.

At this time, by adding AAAA records in the DNS server, PortalServer and ApplicationServer, which are the subjects of protocol conversion in the reverse proxy, will be able to provide IPv6-based application services.

PC terminals on the local government's internal network, with respect to Web access and other proxy settings, will be able to access the IPv6-based Web by designating the DMZ ProxyServer as before.

Table 2.6.4.1: Address Designs for IPv6 Deployment Network Configuration Using Proxy Method

Super Segment	Segment	Network		Address		Source		
		IPv4	IPv6	IPv4	IPv6	Host/Router	Phy. Port	Log. Port
Local gov't network 192.0.2.0/27 2001:db8:1000::/48	External connection segment	192.0.2.0/30	2001:db8::/64	192.0.2.2	2001:db8::2	RouterA	eth2/0	eth2/0
	Pre-border segment	192.0.2.8/29	2001:db8:1000:10::/64	192.0.2.9	2001:db8:1000:10::1	RouterA	eth2/1	eth2/1
				192.0.2.10	2001:db8:1000:10::2	FW1	eth1	eth1
	DMZ segment	192.0.2.16/29	2001:db8:1000:50::/64	192.0.2.17	2001:db8:1000:50::1	FW1	eth2	eth2
				192.0.2.18		MailServer	fa1	fa1
				192.0.2.19	2001:db8:1000:50::19	ProxyServer	fa1	fa1
				192.0.2.20	2001:db8:1000:50::20	DNSserver	fa1	fa1
	Post-border segment	10.1.100.0/24		10.1.100.1		FW1	eth3	eth3
				10.1.100.2		RouterB	eth0/0	eth0/0
	Internal client segment for external connection	10.1.110.0/24		10.1.110.1		RouterB	eth0/1	eth0/1
				10.1.110.101		PC1	fa	fa
				10.1.110.102		PC2	fa	fa
				10.1.110.201		PC3	fa	fa
	Internal server segment for external connection	10.1.120.0/24		10.1.120.1		RouterB	eth0/2	eth0/2
				10.1.120.2		FW2	eth1	eth1
				10.1.120.100		AdminServer	fa1	fa1
				10.1.120.101		PortalServer	fa1	fa1
				10.1.120.102		ApplicationServer	fa1	fa1
	External database segment	10.1.130.0/24		10.1.130.1		FW2	eth2	eth2
				10.1.130.2		DataBaseServer	fa1	fa1
	Internal database segment	10.1.230.0/24		10.1.230.1		DataBaseServer	fa2	fa2
				10.1.230.2		FW3	eth1	eth1
	Private internal server segment	10.1.220.0/24		10.1.220.1		FW3	eth2	eth2
				10.1.220.2		RouterC	eth2/0	eth2/0
				10.1.220.100		AdminServer	fa2	fa2
				10.1.220.101		JudgeServer	fa1	fa1
	Private internal client segment	10.1.210.0/24		10.1.210.1		RouterC	eth2/1	eth2/1
				10.1.210.101		PC4	fa	fa
				10.1.210.102		PC5	fa	fa
	FW/IDS operation management segment	10.1.500.0/24		10.1.500.1		FW1	eth4	eth4
				10.1.500.2		FW2	eth3	eth3
				10.1.500.3		FW3	eth3	eth3
				10.1.500.4		IDS	fa	fa
				10.1.500.11		FW Console	fa	fa
				10.1.500.12		IDS Console	fa	fa

Points of Caution in the Proxy Method

Here we provide some points concerning minimum considerations that should be addressed in performing IPv6 deployment using proxies. These points are based on examples of network construction utilizing proxy servers that support IPv4/IPv6 translation in local government networks.

(1) Protocol conversion settings

In setting the reverse proxy server, simply introducing an IPv4/IPv6-compliant proxy server will make it possible to realize protocol conversion with almost the same settings used in the existing IPv4-based proxy settings. In other words, it is simply a matter of adding Listen registration for capturing corresponding packets and also adding IPv6 address base registration together with the IPv4 address base. In actuality, rather than converting IPv6 packets into IPv4, the IPv4/IPv6 packets are supplemented and transferred statically on an IPv4 packet base.

Concerning reverse proxies, normally one reverse proxy server is installed to support one (one type of) server. Like the use scenario shown in Figure 2.6.4.1, however, there are also cases when agent responses of multiple servers (Web portal server and electronic request server) are realized with one reverse proxy server (one IP address). In these cases, the reverse proxy server recognizes the destination server based on the domain name specified in the URL. In cases such as these, there is no particular problem to use Apache-2 in successfully performing IPv4/IPv6 translation.

(2) Processing capability

As described in "Protocol conversion settings," rather than performing any special processing compliant with IPv6, since the proxy server just allows IPv6 send/receive processing combined with IPv4 packet send/receive processing as an existing proxy function, to use this in actual operation, there is no significant degradation from the existing proxy server processing capability.

(3) Co-existence with the existing proxy server

Depending on the existing proxy server, there are cases in which they cannot be easily replaced if they contain special functions and settings. On the other hand, if IPv6-compliant proxy software is loaded in a universal proxy, it is possible to realize protocol conversion that has a uniform level of processing capability at relatively low cost.

Thus, in realizing IPv6 deployment with the proxy method, as shown in Figure 2.6.4.3, the existing proxy server and the IPv6-compliant proxy server are made to co-exist, and by registering A records and AAAA records in the DNS, operation that uses the existing proxy server or the IPv6 proxy server as needed is possible. If the configuration is designed so that the existing IPv4-based access uses the existing proxy server and only the IPv6-based access uses the newly-installed low-cost IPv6-compliant proxy server, it is possible to achieve a balance between stability and cost performance.

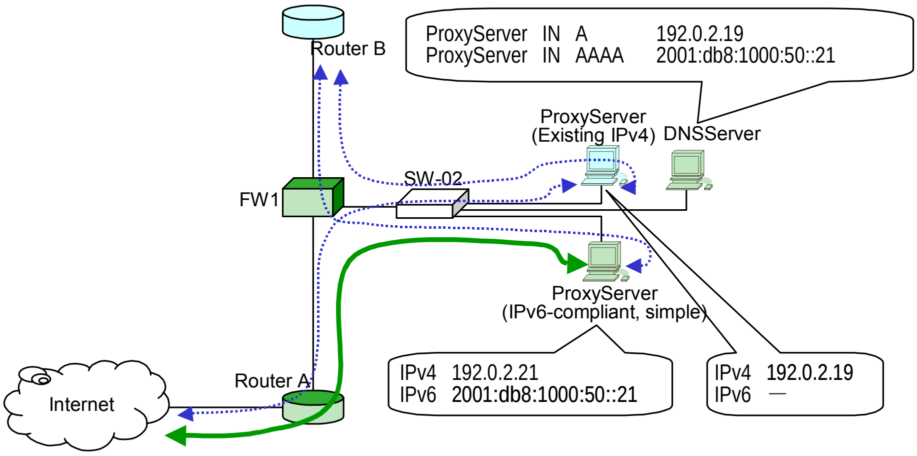


Figure 2.6.4.3: Separate Uses of the Existing (IPv4) Proxy and the IPv6-compliant Proxy

2.6.5 Case of IPv6 Deployment Using Dual Stack Method

Configuration Overview

An overview of a configuration for a local government network using the dual stack method of IPv6 deployment is shown in Figure 2.6.5.1.

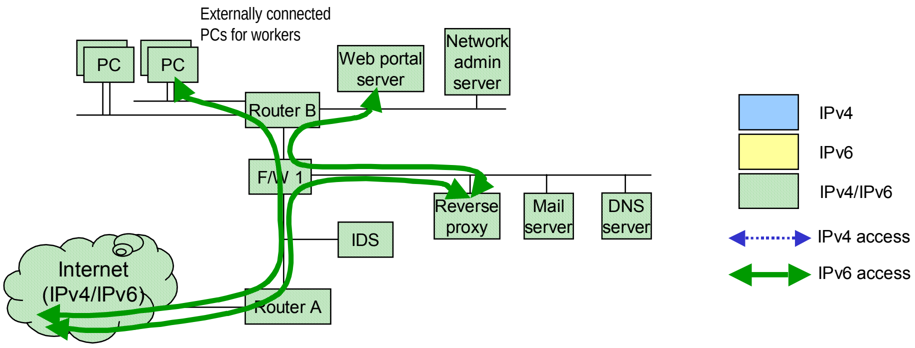


Figure 2.6.5.1: Configuration Overview of IPv6 Deployment Using Dual Stack Method

This method of IPv6 deployment brings both the IPv4 and IPv6 protocols to all devices configured on the network. IPv4 and IPv6 network settings can be made independently, and there is basically no mutual interference between protocols. (See section 2.3.1, "(2) Impact on Existing IPv4 Network Services.") Smoother IPv6 deployment is possible when the overall network is migrated to an environment in which either IPv4 or IPv6 can be used. The operational and cost burden, however, for making the entire network IPv6 compliant is greater.

Due to the features of the dual stack method that bring IPv4 and IPv6 compliance to all network devices, and since there is a larger cost burden in introducing these protocols for the entire existing network, the IPv6 deployment patterns being assumed are mainly of the independent merging type. If the dual stack method is to be applied in the staged replacement type of deployment, the network can be changed to the dual stack method after the translator method, reverse proxy method, tunnel method and other methods are used in the initial stage to bring real IPv6 compliance to the network devices being operated.

Example of Dual Stack Method Application in the Model Case

Figure 2.6.5.2 shows a concrete network configuration where the overview configuration shown in Figure 2.6.5.1 is applied to the model case. In addition, a directory of address designs supporting this network configuration is given in Table 2.6.5.1. For information on basic components, see Table 2.6.1.1 (above).

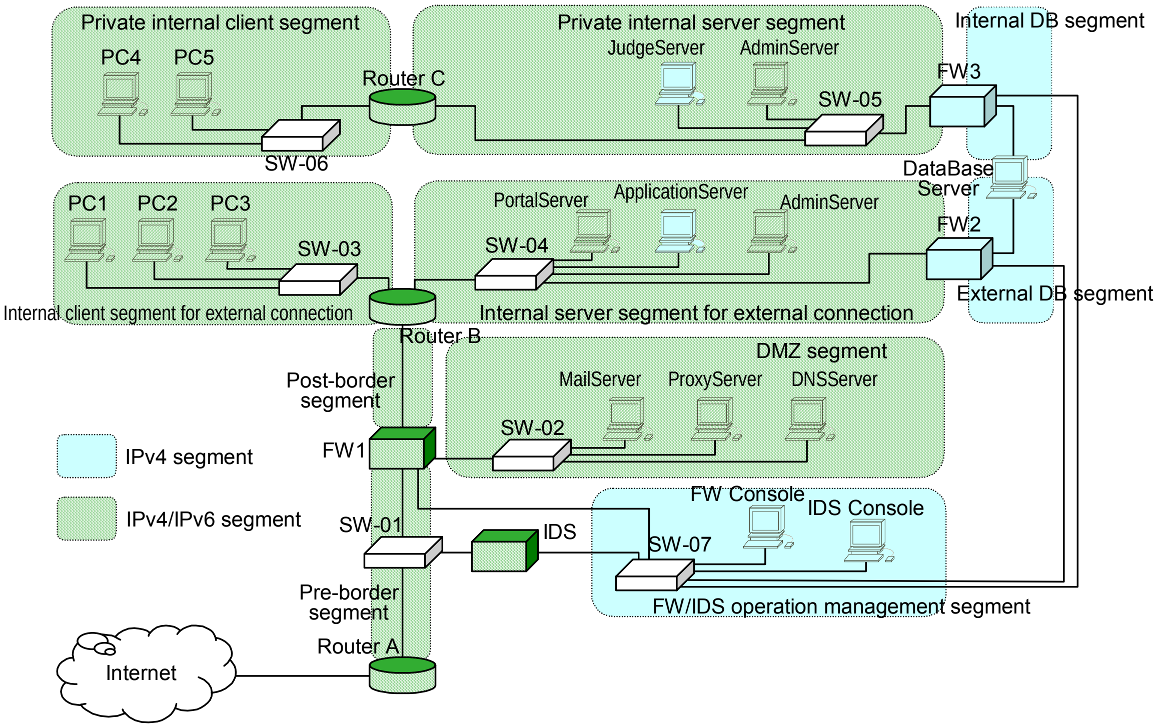


Figure 2.6.5.2: IPv6 Deployment Network Configuration for Model Case Using Dual Stack Method

The network configuration shown in Figure 2.6.5.2 is an example that attempts to bring IPv6 compliance to the entire network without using tunnels or translation. In this network, all user segments can communication directly in IPv6.

Devices that are either difficult or impossible to migrate, such as legacy application servers or segments that operate/manage security devices, are left as is in IPv4. User PC terminals and other devices that do not support IPv6 can also be connected.

Table 2.6.5.1: Address Designs for IPv6 Deployment Network Configuration Using Dual Stack Method

Super Segment	Segment	Network		Address		Source		
		IPv4	IPv6	IPv4	IPv6	Host/Router	Phy. Port	Log. Port
Local gov't network 192.0.2.0/27 2001:db8:1000::/48	External connection segment	192.0.2.0/30	2001:db8::/64	192.0.2.2	2001:db8::2	RouterA	eth2/0	eth2/0
	Pre-border segment	192.0.2.8/29	2001:db8:1000:10::/64	192.0.2.9	2001:db8:1000:10::1	RouterA	eth2/1	eth2/1
				192.0.2.10	2001:db8:1000:10::2	FW1	eth1	eth1
	DMZ segment	192.0.2.16/29	2001:db8:1000:50::/64	192.0.2.17	2001:db8:1000:50::1	FW1	eth2	eth2
				192.0.2.18	2001:db8:1000:50::18	MailServer	fa1	fa1
				192.0.2.19	2001:db8:1000:50::19	ProxyServer	fa1	fa1
				192.0.2.20	2001:db8:1000:50::20	DNSserver	fa1	fa1
	Post-border segment	10.1.100.0/24	2001:db8:1000:100::/64	10.1.100.1	2001:db8:1000:100::1	FW1	eth3	eth3
				10.1.100.2	2001:db8:1000:100::2	RouterB	eth0/0	eth0/0
	Internal client segment for external connection	10.1.110.0/24	2001:db8:1000:110::/64	10.1.110.1	2001:db8:1000:110::1	RouterB	eth0/1	eth0/1
				10.1.110.101	2001:db8:1000:110::101	PC1	fa	fa
				10.1.110.102	2001:db8:1000:110::102	PC2	fa	fa
				10.1.110.201	2001:db8:1000:110::201	PC3	fa	fa
	Internal server segment for external connection	10.1.120.0/24	2001:db8:1000:120::/64	10.1.120.1	2001:db8:1000:120::1	RouterB	eth0/2	eth0/2
				10.1.120.2	2001:db8:1000:120::2	FW2	eth1	eth1
				10.1.120.100	2001:db8:1000:120::100	AdminServer	fa1	fa1
				10.1.120.101	2001:db8:1000:120::101	PortalServer	fa1	fa1
				10.1.120.102		ApplicationServer	fa1	fa1
	External database segment	10.1.130.0/24		10.1.130.1		FW2	eth2	eth2
				10.1.130.2		DataBaseServer	fa1	fa1
	Internal database segment	10.1.230.0/24		10.1.230.1		DataBaseServer	fa2	fa2
				10.1.230.2		FW3	eth1	eth1
	Private internal server segment	10.1.220.0/24	2001:db8:1000:220::/64	10.1.220.1	2001:db8:1000:220::1	FW3	eth2	eth2
				10.1.220.2	2001:db8:1000:220::2	RouterC	eth2/0	eth2/0
				10.1.220.100	2001:db8:1000:220::100	AdminServer	fa2	fa2
				10.1.220.101		JudgeServer	fa1	fa1
	Private internal client segment	10.1.210.0/24	2001:db8:1000:210::/64	10.1.210.1	2001:db8:1000:210::1	RouterC	eth2/1	eth2/1
				10.1.210.101	2001:db8:1000:210::101	PC4	fa	fa
				10.1.210.102	2001:db8:1000:210::102	PC5	fa	fa
	FW/IDS operation management segment	10.1.500.0/24		10.1.500.1		FW1	eth4	eth4
				10.1.500.2		FW2	eth3	eth3
				10.1.500.3		FW3	eth3	eth3
				10.1.500.4		IDS	fa	fa
				10.1.500.11		FW Console	fa	fa
				10.1.500.12		IDS Console	fa	fa

Points of Caution in the Dual Stack Method

Here we provide some points of caution concerning the establishment of dual stack as a basic policy for IPv6 deployment. These points are based on examples of local government network construction utilizing the dual stack method.

Since dual stack also supports in part the other methods (tunnel, translator, and proxy), the points of caution concerning dual stack given here applies also to the other methods.

(1) Plug and play

Plug and play is a standard feature with IPv6. In other words, IPv6 itself (on the network layer) is equipped with the Neighbor Discovery Protocol (NDP; see RFC 2461, RFC 2462) as one of its functions, and since IPv6 addresses are therefore automatically set, obviating the need for users to set their own address, the user's burden in setting their terminals can be reduced.

However, since DNS information cannot yet be automatically set at this point in time, complete plug and play is not yet possible. The procedure for automatically setting DNS information has only recently been standardized (RFC 3315, RFC 3646), and it has not yet reached a practical stage. For the time being, DNS information must be set either by using the automatic IPv4-based DHCPv4 setting procedure or making individual settings manually[6].

(2) Terminal management

Automatically generated IP addresses are normally stateless (status not maintained) addresses. In other words, while the network prefix (upper 64 bits) portion of the IPv6 address is automatically advertised from the router representing network segment of the connection destination based on the NDP, the interface identifier (lower 64 bits) is automatically generated by MAC addresses assigned to the NIC of each terminal based on EUI-64 rules; addresses are not managed in any particular manner. Since interface identifiers can be freely set so long as they are not duplicated among terminals within the same segment, depending on the IPv6 address itself, caution is advised, as complete terminal management is not possible. The fact that complete terminal management with an IP address is not possible is the same as IPv4 in the aspect that the user can freely set their own IP address.

Though complete terminal management procedures have not yet been established at this time, with the introduction of IEEE 802.1x for use in terminal authentication in the future, it will probably be possible to manage terminals and restrict access.

[6] Windows XP currently supports only IPv4 DNS queries.

(3) IPv6 Server DNS Registration

While it is possible for IPv4 and IPv6 to basically co-exist on the same network infrastructure, in services that utilize DNS name resolution, for example, the deployment of IPv6 may indirectly bear an adverse impact on IPv4 services.

In other words, if AAAA records of a server that does not yet fully support IPv6 are carelessly registered in the DNS, it is possible that IPv4 access responses may be significantly delayed. This is because general Web browsers place priority on IPv6 during domain name resolution and it takes time to confirm IPv6 communication failures when IPv6-based server access occurs first and there is no response in IPv6.

In the process of switching the server to IPv6, it is probably best to implement AAAA record registration to the DNS server after first confirming that IPv6 is operating normally.

2.7 Evaluations

In this section, we evaluate the various results that were obtained from the IPv6 deployment of the model case shown in Figure 2.6.2.1 based on the four typical types of deployment.

2.7.1 Evaluations from the Constructor's Perspective

In the dual stack configuration in particular, since IPv6 settings are required in addition to IPv4, it is said that as many as twice as many operations are easily required, but in actually having built a configuration, we found that in configurations of address settings, routers, servers and other devices, it is possible to handle most settings simply by setting IPv4 and IPv6 to "pair." The router and server functions also have no problems running, and even if there are twice as many settings to make, in actuality, the extra burden involved is relatively low.

Though this may rely on the model of device being used, in using 6to4 or ISATAP dynamic tunnels or making router settings for static tunnels for the tunnel method of IPv6 deployment, settings can be made in a relatively easy process. However, since unexpected problems can occur as a result of applications that cannot communicate due to tunnel packets being filtered in an existing IPv4 router or other device, or that cannot recognize the virtual tunnel interface at the client terminating the tunnel, sufficient advance verification needs to be conducted before this configuration is used.

If translation is required, proxy server settings in the proxy method can be relatively easy to make. In the translator method, however, since DNS proxy settings, pool address designs and other areas are relatively complex in addition to the translator itself, the aims of translation must be clearly defined and then the design must be carefully studied in advance.

IPv6 addresses contain four times as much information compared to IPv4 addresses, making it difficult for users to have intuitive images of them or remember them. Specifically, users feel some resistance in such cases when analyses related to client terminals that automatically generate interface identifiers in EUI-64 are conducted. Automatic generation by EIU-64 should be avoided by all means for routers, servers, and other devices other than user terminals, and simple, easy-to-understand interface identifiers should be set manually.

From the aspect of actual address design, however, for example in cases where /48 IPv6 prefixes have been assigned, the ability to effectively use 16 bits, i.e. four hexadecimal characters, can be considered an advantage. Compared to the case of

IPv4 where addresses are designed while estimating the future number of terminals to be connected to each network segment, in practice, IPv6 is extremely convenient, as addresses can be designed in accordance with the network design at the prefix section and no consideration needs to be given at all to the number of terminals that will be connected to each segment. Also, even in instances where unexpected additions or changes occur in the network configuration, compared to IPv4 where NAT must be applied or otherwise the existing assignment of addresses must be changed, a major advantage with IPv6 is that IPv6 can handle these adjustments very easily. Putting it the other way around, in the IPv6 address design that has an abundance of address space, it can be said that simple, flexible, easy-to-understand address designs need to be implemented from the initial stage in order to accommodate future changes in the network configuration.

2.7.2 Evaluations from the Operator's Perspective

At the present time, to operate and manage IPv6 and also to continue running existing applications, it is necessary to manage the normal operation of both IPv4 and IPv6. In the IPv4/IPv6 dual stack environment, the number of steps to operate and manage a layer 3 network is no small matter and the burden increases. In addition, with respect to network management tools that remotely monitor the normal operation of devices, all conditions and other matters -- since the number of devices IPv6-related MIB is increasing and the SNMP transport for most devices does not yet support IPv6 -- a dual stacking environment with IPv4 is indispensable.

Concerning IPv6 QoS control functions, at the present time, advanced QoS control utilizing flow labels has not yet been realized in IPv6-compliant routers, although QoS control functions equivalent to IPv4 can be used. As a realistic method of using QoS control on a government network, although it is possible that QoS settings based on specific IP addresses or application types may be required to secure communications bands, in practice, sufficient settings are also possible in IPv6, and we were able to confirm that the functions work effectively.

In local government and other user networks, due to the relatively long equipment replacement cycles, we expect that uneven processing capabilities among devices on the overall network system will occur in the process of IPv6 deployment. In the example in Figure 2.6.2.4, the processing capabilities of Router A and FW1 are relatively high, while the lower processing capability of the ISATAP router realized in the general-purpose server causes a bottleneck. While it is necessary in such cases to set QoS controls for each type of application (real-time types, file transfer types, etc.), it is not possible to sufficiently realize priority control over packets in the general-purpose server, causing problems in managing traffic. In our attempt at IPv6 deployment using the tunnel method, we considered applying priority control to traffic being transferred to the ISATAP router that was becoming the bottleneck, and in another router, Router A, where QoS control was sufficient, we were able to indirectly control the QoS of the bottleneck server by incorporating detailed QoS settings for each application.

2.7.3 Evaluations from the User's Perspective

From the aspect of enabling users to basically be unaware of IPv4/IPv6 when they operated an IPv6-compliant terminal (running Windows XP), we confirmed that there were no problems in such areas as automatically generating IPv6 addresses or basic network functions, and that they reached a sufficient standard.

Concerning basic settings and our status checks on IPv6-related network parameters and ICF (personal firewall), while all support only exists in the command line interface, the basic functions have IPv4-level support, so it is doubtful that the user will experience any particular inconvenience. From now on, we expect that the following issues concerning the detailed use environment will be resolved:

- Support for the literal IPv6 address format for URL input in the Internet Explorer Web browser
- Support for DNS query IPv6 transport
- Realization for automatic address settings that include DNS information

2.7.4 Evaluations concerning Deployment Costs

In newly installing network devices that support IPv4/IPv6 dual stack, there are almost no differences among products not yet supporting IPv6 and in cost. If software needs to be upgraded or otherwise in order for it to support IPv6, however, there may be an associated cost depending on the product, so each product needs to be studied and evaluated.

In IPv6 deployment patterns of the staged replacement type, IPv6 deployment cost savings can be realized by replacing devices with IPv6-compliant devices on those occasions where devices are periodically replaced for maintenance. As a basic approach, since it is expected that the need for IPv6 compliance will grow over time, even if it is not immediately necessary to introduce IPv6 compliance when devices are replaced for maintenance, it is probably best to introduce IPv6-compliant devices at this time anyway. With devices such as firewalls and routers for external connection, however, these devices should be changed over to IPv6 compliance as first priority in the IPv6 deployment process, irrespective of their periodic replacement schedule, a task that will generate considerable cost.

In the IPv6 deployment patterns of the independent merging type, in principle, there will be a cost for all newly introduced equipment, so these costs should be positioned as advance investment in network infrastructures that are expected to support broadband in the future. Thus, when selecting IPv6-compliant devices to be used in the independent merging type of IPv6 deployment, sufficient consideration needs to be given to future operation requirements.

2.7.5 Tips

Commercial IPv6-compliant devices such as routers, servers, and terminal OS are becoming quite sophisticated. We have also confirmed that their functions operate at a sufficient level of stability, including mutual compatibility. IPv6 compliance in security-related devices, however, is progressing relatively slowly, and this has been a large obstacle inhibiting IPv6 deployment. Here we present the results of our evaluations from empirical experiments concerning firewalls and IDS.

<IPv6-compliant firewalls>

Though IPv6-compliant firewalls have been publicly available since about April 2003, at the present time, they have not yet become very widespread. We verified the operation of functions in the IPv6-compliant Nokia IP350 (Firewall-1) and we confirm that there have been no problems concerning the basic packet filtering function at least in layer 3 and layer 4.

In a more detailed use environment, however, the following problems and areas of inconvenience remain:

- In obtaining an IPv6-compliant license, a unique license application that is different from IPv4 is required.
- The management of objects used in the Policy (security rules) has been divided between IPv4 and IPv6, and management of IPv4 and IPv6 dual stack servers and other devices is complicated.
- Logs for IPv4 and IPv6 cannot be checked on the same screen.
- It is not possible to set the filter so that filtering is based on information contained in the tunneling packets.
- Though a function for linking to a specified IDS is claimed, the linking capability is not sufficiently developed.

- The IPv6-compliant multicast routing protocol is not yet supported.

None of these points, however, is serious, and this firewall is sufficiently usable. A more sophisticated filtering function for tunnel packets and other functions is expected in the near future.

<IPv6-complaint IDS>

At the present time, there are no other IPv6-compliant IDS products other than a firewall. We verified the operation of IPv6-compliant IDS functions in the IIS Proventia A604. Though we were able to confirm that the basic IDS function -- the detection capability -- was equivalent to IPv4, in a more detailed use environment, the following issues and problems remain:

- Though support for IDS IPv6-over-IPv4 tunneling communications is claimed at the current stage, it only detects whether or not a tunneling communication exists and it does not yet fully support detection of packet contents.
- Though it seems that, in IPv6 communications of IDP function control in IDS, the RSKILL function is working on the log, we observed in actuality that the reset function does not work normally.
- Though the trigger conditions in the FW/IDS security breach messaging function support both IPv4 and IPv6, communication with the mail server occurs only in IPv4.

Like the firewall, however, none of these points is serious, and these functions are sufficiently usable. Greater IPv6 support for additional functions is expected in the near future.

2.8 Issues

2.8.1 Multicast-related

Concerning efforts to realize multicast streaming services, since the firewall at the present time does not support IPv6-compliant multicast routing protocol (PIM-SM), it is not possible to realize multicast streaming services to the local government's internal LAN segment for external connection just with a network configuration like the one shown in the model case. Basically, IPv6 multicast protocol support for the firewall is desired for the future.

Beyond multicast streaming, however, we are expecting that a variety of broadband applications will be introduced along with IPv6 deployment in the future. If these application introductions are to be supported on the conventional concept of network operation, it will no doubt become necessary in the future to provide vastly greater processing capability, diverse functions, and IPv6 support for these areas. In the network configuration that we used in the model case, in our effort to realize multicast streaming reception from the content server installed in the external segment to the local government's internal LAN segment for external connection, as a temporary measure to solve the problem of the firewall's lack of support for IPv6 multicast, we added a direct multicast-dedicated path between Router A and Router B without passing through the firewall. There may be some negative evaluations in a measure like this concerning security management in actual operation. However, in studying the introduction of a variety of applications from now on in local government networks, it is not absolutely necessary to adhere to the fixed concept that "all communications packets must pass through a firewall." Rather, we believe flexible network design is also required.

2.8.2 Security Policies

In section 2.3.2, "Network Security Policies in the Initial Stage of IPv6 Deployment," we tentatively presented relaxed and strict models of security policies in the initial stage of IPv6 deployment. From now on, however, for IPv6 to achieve full-scale penetration, we believe it is necessary to establish typical security policies.

Rather than having fixed and complete security policies that apply to all networks, we are assuming security policies that should take on a variety of patterns based on physical conditions of the network, operating conditions, and the ideas of administrators. The most important overriding point is that a practical introduction of IPv6 should be tried, and that security policies should be gradually adjusted based on feedback concerning a wide range of problems so that ideal policies can be achieved where possible. From this perspective, in the initial stage of IPv6 deployment patterns of the independent merging type and before actual operation of the new IPv6 network starts, the policies should be actively tried and verified.

2.8.3 Redundant Configurations

In local government networks, full-scale introduction of redundant networks is rare, and realistic measures toward redundancy, such as duplicating only vital equipment in certain sections or manually switching to a spare device assuming service stoppage for a fixed period of time, are adopted. Part 2 does not directly cover redundant configurations. However, as services relying on IPv6 networks continue to become more sophisticated, we believe that demand for measures toward redundancy will grow.

2.8.4 Co-existence of Firewalls and IPsec

Besides the ability of two terminals to engage in direct end-to-end communications with each other, a major feature of IPv6 is the ability of these terminals to realize secure communications by generating a direct IPsec tunnel. In this model case, we were able to verify that IPsec could be used via relatively simply operations by the user, including terminal authentication in IKE, when an external IPv6 terminal and an internal IPv6 terminal use an IPsec communications tool (MyNetManager). When IPsec communications is used, however, due to filter settings in the firewall installed at the border of the local government network, IPsec packets are allowed to be transferred unconditionally, an issue that still remains to be resolved.

If uniform access restrictions based on organization-defined security standards are required, like local government networks, there is a need for a way to manage whether encryption should be enabled or disabled between terminals. At present, no effective solution to this problem exists, and it is an issue that needs to be resolved very soon as IPv6 is introduced on local government networks. Below, we offer proposals aimed at realizing co-existence of a firewall and IPsec.

<Basic policies for support measures>

The following two approaches are possible ways to achieve co-existence of a firewall and IPsec:

- Border decryption

  A firewall interpositioned on the communications path between the two terminals uses some way to obtain a key to decode the IPsec packet, filter it, and then to re-encrpyt allowed packets for transmission to their destination.

- Personal firewall
  Instead of filtering by a border area firewall interpositioned on the communications path between the two terminals, personal firewalls mounted on the terminals filter packets that have not been subject to IPsec.

Considering the advantages and disadvantages of the above two approaches, especially the burden of encryption/decryption required by the firewall, we believe that in practice, the personal firewall approach is more realistic.

<Relationship between the personal firewall and IPsec module>

The personal firewall cannot always unconditionally filter packets without being aware of IPsec. At present, the IPsec processing module that is implemented is in some cases positioned in a protocol stack manner on the outside of the personal firewall, and in these cases, the same problems as those of a border area firewall occur. Results of our investigations show that there are no problems with Windows XP-based implementations (combination of Windows XP standard IPsec and ICF[7] or of MyNetManager and ICF), but the problems mentioned above occur with Linux OS.

<Linking the border firewall and the personal firewall>

If packet filtering is possible at the personal firewall without being influenced by IPsec encryption, a next stage would require linking the personal firewall with the border firewall and filtering packets based on organization-defined security policies. To achieve this sort of function, it would probably be necessary to install a separate server (hereafter referred to as the "policy manager") capable of centrally managing the settings of border firewalls or personal firewalls installed in terminals on the entire network. The main functions required by this sort of policy manager are given below:

- The policy manager can remotely control the personal firewall settings of all terminals connected to the network being managed.
- The policy manager can recognize terminals adhering to controls from the policy manager and can remotely control settings of border firewalls so that access to these terminals is allowed according to uniform standards.
- Conversely, the policy manager can also recognize terminals that do not adhere to controls from the policy manager and can remotely control settings of border firewalls so that access to these terminals is blocked according to uniform standards.
- When the administrator simply sets network security policies in the policy

[7] Internet Connection Firewall: Supports IPv6 using Advanced Networking Pack (KB817778).

manager, the policy manager can interpret the content and control the settings of individual border firewalls and personal firewalls, and network security policies set by the administrator can be applied across the entire network.

- In principle, users are not allowed to modify personal firewall settings on their terminals. If user-defined settings are allowed, the policy manager will be able to recognize those settings.

3. Guideline for Large Enterprise Segment

3.1 Outline

3.1.1 Definition

Here we explain the definition of the large enterprise that Part 2 is targeting. The target in the large corporate segment is the corporate intranet of a certain scale. Its features are as follows:

- The overall network is operated and administered by a dedicated division.
- It is a comparatively large network having more than several tens of users and several bases that are connected through a WAN.
- There is an intranet within the organization.
- Application services such as mail and the Web are provided within or beyond the organization.

(For the above items see page 6 of the IPv6 Promotion Council of Japan [http://www.v6pc.jp/] Deployment Working Group's Large Enterprise and Local Government Segment Guidelines [hereafter referred to as Large Enterprise / Local Government Guidelines].)

3.1.2 Aim of this Guideline

Part 2 is intended to model an ordinary large enterprise network and to provide guidance for migrating from an existing IPv4 network to an environment that can use high-grade IPv6 applications. Empirical experiments, in which selected network structures were actually constructed as models, verify the validity of actually changing the router and server devices from an IPv4 environment to an IPv6 environment. The results of evaluation from various aspects including construction, operation and migration costs have made this quite clear and have demonstrated the know-how related to making the change.

Part 2 is aimed at members of information system divisions who are involved in constructing and administering large enterprise networks, systems integrators and IPv6 application developers.

3.1.3 Deployment Scenarios for Large Enterprise Networks

(1) Triggers for deployment

We believe the triggers for the decision for the IPv6 deployment of a large enterprise network fall into the following two patterns:

- Advance deployment of the IPv6 network environment
  This pattern prepares for prompt deployment when network applications with a promising future have appeared by deploying IPv6 beforehand on the basis of a long-term equipment plan.

- Deployment of IPv6 together with the introduction of new applications
  This pattern improves working efficiency on business trips or at meetings, or achieves better working cooperation in work at home by deploying IPv6 and new applications at the same time.

Presumably the former is determined by top-down decision-making in cases where future benefits are recognized, and the latter is based on bottom-up decision-making in cases where an immediate benefit is recognized.

In the latter case, there is no presumption that new applications will be introduced with the initial deployment of IPv6. However, if we assume that some applications would be changed as a test when IPv6 is deployed beforehand, it is possible that the latter includes the former. The experimental know-how gained by assuming the latter can probably be applied to the former. Part 2 thus assumes that the latter is the trigger for deployment.

(2) Handling existing IPv4 network services

We shall assume that the networking functions of working applications currently in operation in a large enterprise network are based on IPv4 specifications. While these existing working applications are in use, it is essential to migrate to IPv6 while the IPv4 connection services are being provided. Therefore, in deploying IPv6, we shall construct an IPv4/IPv6 dual stack network in the initial stage with a view to continuing the services that use the existing IPv4 network. Since the present IPv6-compatible networking devices are basically dual stack compatible, this means that the field in which IPv6 can be used will expand as the field of applications for IPv4/IPv6 dual stack expands and IPv4 services will also be continued.

Concerning IPv4 services up to now, if priority control is being applied, it will be necessary to consider priority control of IPv6 traffic in the process of making the dual stack. Moreover, if priority control is not being applied, there must be feedback to the design capacity of the entire network by evaluating quality as a best effort service.

(3) Deployment scenarios

In the case of the pattern of deploying IPv6 in conjunction with the introduction of new applications in a large enterprise, we believe there are the following two scenario patterns for migrating to IPv6. (Large Enterprise / Local Government Guidelines, page 11)

- Staged replacement type

  IPv4/IPv6 dual stack network will be constructed in sections within the intranet of the large enterprise network. IPv6-over-IPv4 tunneling is used for IPv6 communication in order to make an IPv4/IPv6 dual stack sub-network in the IPv4 network.

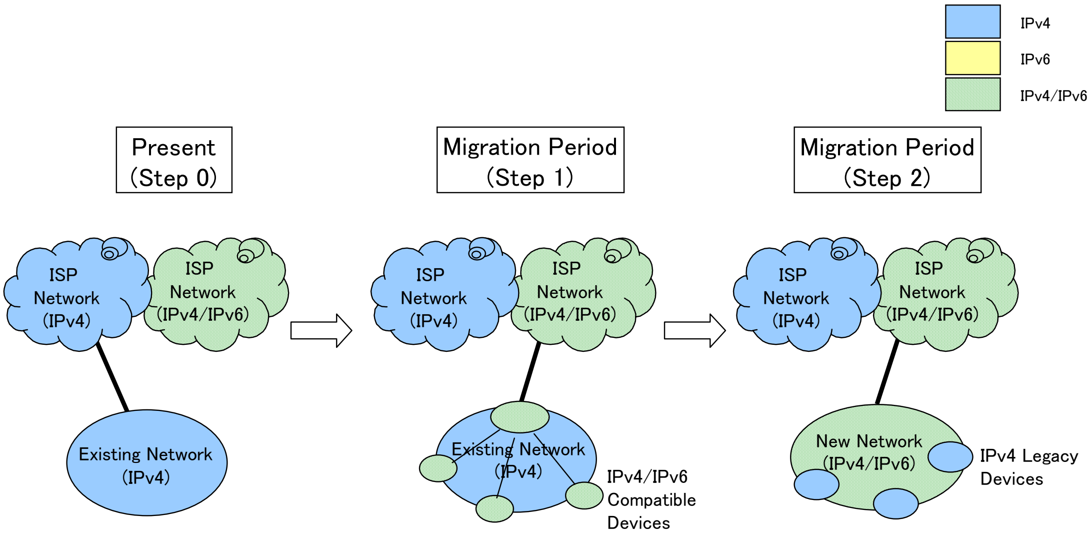


Figure 3.1.3.1: Staged Replacement Type

Step 0: The network is configured only with IPv4.

Step 1: Part of the equipment is IPv6-compatible, and IPv6-compatible devices are assumed to be connected via IPv6-over-IPv4 tunneling.

Step 2: The network is assumed to be an IPv4/IPv6 dual stack.

- Independent merging type

  An IPv4/IPv6 dual stack network is constructed in sections apart from the existing intranet facilities of the large enterprise network. Duplicate facilities will be needed initially, but the former intranet will be gradually intensified on the IPv4/IPv6 dual stack network side and will migrate to IPv6.

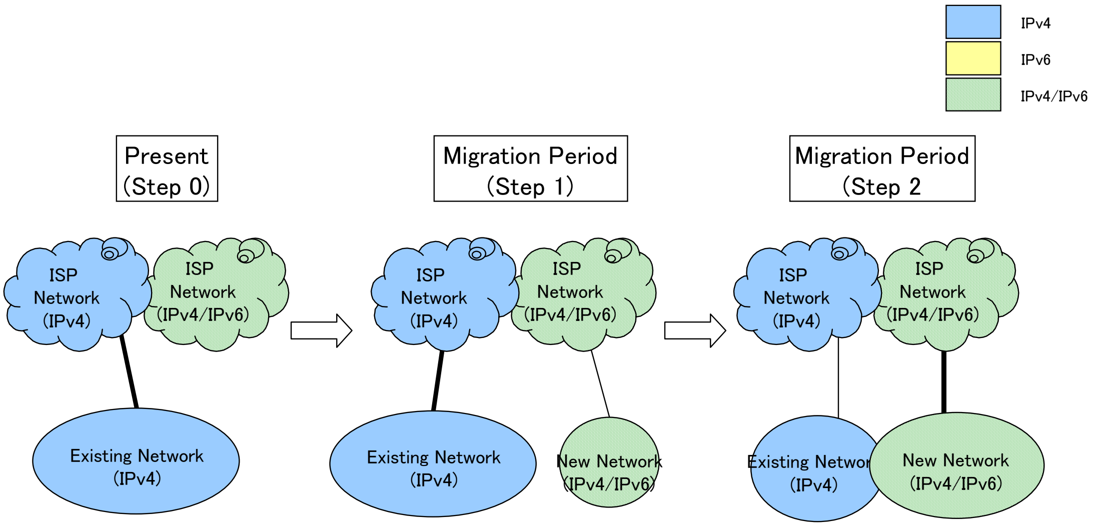


Figure 3.1.3.2: Independent Merging Type

Step 0: The network is configured only with IPv4.

Step 1: An IPv6 network is created independently, and an IPv4/IPv6 dual stack network is assumed to coexist in parallel.

Step 2: We assume the intranet will be concentrated on the IPv4/IPv6 dual stack.

The staged replacement type will operate by flowing the new IPv6 traffic on the present network. Cost increase factors would be replacement or upgrading with IPv4/IPv6 dual stack compatible equipment and the human resources to manage the IPv4/IPv6 dual environment. With respect to equipment costs, if IPv4/IPv6 dual stack compatible equipment were to be deployed at a time when obsolete devices are due for replacement and that timing were to coincide with the introduction of new applications, the cost increase would probably be insignificant. Therefore, the introduction of new applications and the replacement of obsolete equipment must be a planned operation.

With the independent merging type, on the other hand, since the addition of a separate segment is involved, the initial investment in both equipment costs and human resources is required in duplicate. By way of compensation, it has the advantage of offering an IPv6 usage environment in a form that does not impact on the former network services. In the present business networking environment, the provision of duplicate facilities is not generally possible. From this we assume that a pattern of the staged replacement type will enable the investment cost in Part 2 to be held down.

(4) Network security policy

The way security is regarded in large enterprise networking is tending towards greater reliability with respect to business networking, and due to the increasing seriousness of security issues, we believe the trend will become increasingly severe. Meanwhile, as with IP phone, peer-to-peer connection tools are becoming popular, and there is a rising demand for improving connectivity to networks for achieving flexible communication. We believe there is a need for a high level of compatibility of security and flexibility like this in the IPv6 deployment stage. The following two points may be models to satisfy conditions such as this.

- Relaxed model
  Adding an IPv6 packet forwarding setting to the current firewall setting enables the bare minimum connection to be made. In this case, the network administrator passes only authorized traffic though the firewall and security is ensured.

- Strict model
  An IPv6 environment is deployed within the business while the security of the former environment is ensured by not approving a connection between the network in current use and the IPv6 network. In this case, security is ensured by the PC of the network in current use and the PC of the IPv6 network not both using the same facilities.

The relaxed model, in which the PC using the current IPv4 application and the PC using the new IPv6 application can coexist on the same intranet, seems to be the model for a large enterprise.

On the other hand, the strict model seems to be a model in which the network administrator does not allow any flow of traffic that poses a threat to the security of the existing network environment. Since the PC of the existing network and the PC of the IPv6 network are used separately, this is not an ordinary environment for the user. From now on, connection to the intranet will be approved after confirmation that IPv6-compatible firewall products have been evaluated and records of unauthorized access to the IPv6 network have been fed back.

Part 2 is assuming the construction of the relaxed model, which is considered to be more realistic for the user as a scenario of a large enterprise migrating to IPv6.

3.2 Large Enterprise Model

The configuration in Figure 3.2.1 is taken to be the structure of the network of an ordinary large enterprise.

In the model of a large enterprise, a DMZ (DeMilitarized Zone) is installed to form a barrier between external networks and the company's internal network in order to prevent unauthorized penetration from the inside to the outside or from the outside to the inside.

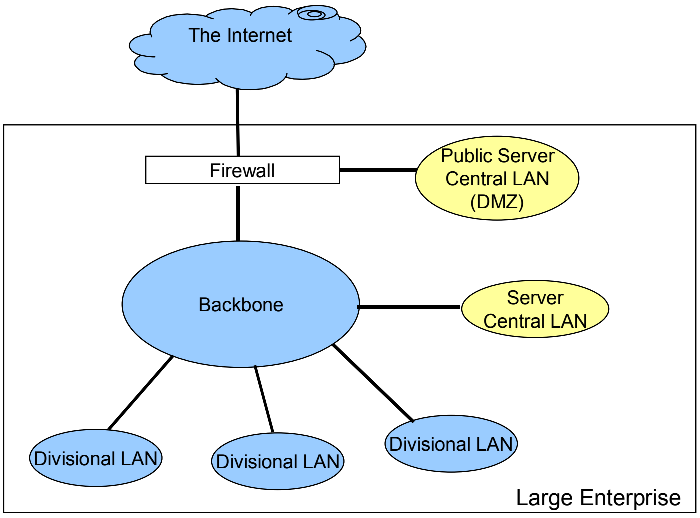


Figure 3.2.1: Large Enterprise Model

3.2.1 Backbone Network

This is the company-wide common backbone administrated by the company's information systems division. It consists of a medium-scale router and small routers and switches. Connections are made to a dedicated LAN within the same site, and dedicated lines, IP-VPN net and wide-area Ethernet are used for remote branch companies and branch offices.

3.2.2 Public Server Central LAN

The public server central LAN, which is administrated by the information systems division, is a network established with a group of servers that can be accessed directly from external networks.

This LAN generally has a Web server, mail server and DNS server to implement services outside the company, and on this occasion we will also adopt this configuration.

3.2.3 Server Central LAN

The server central LAN is established with various servers used within the company, and for the company it is the main network.

Since the company's activities will be affected if trouble has occurred on the network, strict administration and high reliability are demanded.

The servers that establish this LAN include a Web server, mail server and DNS server, as well as various types of application servers used within the company.

3.2.4 Divisional LANs

Mainly PCs are connected to the networks administered by each division. These are used to connect to the company servers and the Internet.

3.2.5 Applications

We assume that applications such as the following will be used by the company model:

- IPv4 working applications: IPv4-compatible applications specific to the work and assumed not to be converted to IPv6.
- Web applications: Various systems that have been developed are based on the use of HTTP and a browser. We assume that servers and clients that have been converted to IPv6 will naturally migrate to IPv6.
- Mail: The most general applications that are used on the basis that they use SMTP and mail clients. We assume that servers and clients that have been converted to IPv6 will naturally migrate to IPv6.
- IP phone (SIP applications): Applications that achieve telephone communication on the IP network. We expect applications that use SIP will become popular and that they will migrate to IPv6.
- Streaming: Applications that transmit real-time and rich content. If multicast is used, its use in the IPv6 environment is seen as being particularly promising.
- Videophone: A typical multimedia application. From now on with the advent of broadband networking, the need to use videophones within the company is likely to increase.

3.3 Consideration of IPv6 Deployment

Here we indicate matters concerning migration of a large enterprise network to IPv6 that should be considered from the viewpoints of the constructor, the operator, and the user.

3.3.1 From the Viewpoint of the Constructor

The constructor must consider whether the services that can be realized by IPv6 and which are demanded by the user can be deployed reliably and efficiently.

(1) Concerning the range of application of IPv6

The range of application of IPv6 presupposes a range of services to be provided by applications that use IPv6. In that case, clarification of conditions such as communication paths and traffic must be considered so that everything can be brought together successfully. Moreover, the deployment of IPv6 driven not only by carrying out the simple essentials but strategically and temporally, there may also be the objective of developing the basis of a new network. These must be considered in determining the range of application of IPv6.

(2) Migration of network

Not only must the migration to IPv6 be realized reliably and efficiently but consideration must be given to doing this without affecting the existing IPv4 services that are currently being provided.

An appropriate network must be constructed after clarifying matters such as communication paths and essential bands so that IPv6 applications traffic will not bring pressure on the existing IPv4 traffic.

(3) Migration of servers

Not only must the construction of servers for IPv6 be realized reliably and efficiently but consideration must be given to doing this without affecting the existing IPv4 services that are currently being provided.

Moreover, administration of their operation must also be considered.

(4) Internet connection

Not only must the IPv6 Internet connection by realized reliably and efficiently but consideration must be given to doing this without affecting the existing IPv4 services that are currently being provided.

In particular, if work has already begun with the definition of private addresses in the initial deployment of IPv6, even later they will need to be reassigned when connection to the Internet is made. Concerning the address system when IPv6 global addresses are used, these must be determined beforehand with the knowledge of the operator.

3.3.2 From the Viewpoint of the Operator

The operator must consider whether to follow the safety (assurance of security) and operating efficiency that were achieved by the IPv4 network or to improve them.

(1) Concerning the administration of users

In an IPv4 network in a large enterprise, IP addresses are generally assigned centrally by the DHCP server. Therefore, this DHCP server administers the correspondence between every user and IP address, and can identify the source if a problem such as a virus occurs.

Similarly, in the case of migration to an IPv6 network, it will also be necessary to prepare for the simple assignment of addresses and the identification of sources of problems that might occur.

(2) Concerning the acquisition of a global address

The time for acquiring a global address must be considered. It is not necessary in the initial IPv6 deployment, but assignment will become necessary when operation has begun with the definition of private addresses and an IPv6 connection to the Internet is made. The time of reassignment is associated with a cessation of the network (and services) so the timing for acquiring a global address must be decided by considering the impact in accordance with the number of work processes involved.

(3) Concerning subnet assignment

As with the IPv4 network, the most suitable address allocation is made in accordance with the network (system) configuration. At this time, in the initial IPv6 deployment, operation begins with the definition of private addresses, and if there is to be reassignment when the IPv6 Internet connection is made, this must be considered so as to make it simple.

Specifically, with respect to the allocation of the remaining 16 bits of the network prefix, if the acquisition is /48, then reassignment can be simplified by defining the global address so that there is no need for change after it has been acquired.

Figure 3.3.2.1 shows an example of a global IPv6 address of /48 having been acquired.

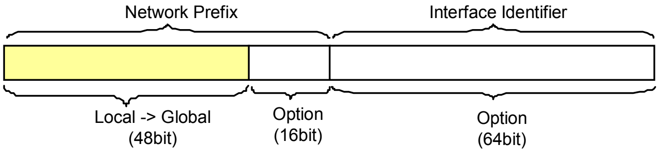


Figure 3.3.2.1: Example of Global IP Address

(4) Concerning the IPv6 public server

If a public server for IPv6 is to be developed, easy management of the content and security must be considered.

The new installation of a public server separate from the one for IPv4 requires that the same content is available in both directions, which complicates administration. Therefore, the public server will be for the IPv4/IPv6 dual stack, and administration is simplified by having the same content referenced.

Moreover, as with the current IPv4 network, security must be ensured by providing transmission to the DMZ and a firewall or similar arrangement.

(5) Concerning security

Consideration must be given to enabling the same security as the IPv4 to be ensured.

Specifically, a firewall or similar arrangement shall be deployed to restrict access from inside and outside the network. Also, terminals are to be defined by global addresses so that they will not be subject to attack, and consideration must be given to the method of allocating the addresses.

3.3.3 From the Viewpoint of the User

With regard to services that are provided under IPv6, consideration must be given to issues of concern to users, such as when and how the service can be used and the assurance of security concerning the use of global addresses.

(1) Concerning the use of applications

We must consider the use of new applications that can be realized by IPv6 and, if it has been decided that applications that are being used under IPv4 will migrate (expand) to IPv6, the details of using the services, the ranges and the development schedules of the services to be provided must be considered.

In particular, depending on the application being used, since the application needs to be aware of whether IPv4 or IPv6 should be used to suit the other party in the communication.

(2) Concerning security

The use of global addresses is a precondition in an IPv6 network. Consideration must be given to the administration of addresses so that terminals will not be identified and become subject to attack.

3.4 IPv6 Deployment Elemental Technologies

IPv6 deployment elemental technologies used for verification with the current migration model on a large enterprise network are shown below.

(1) Tunneling (IPv6 over IPv4)

In communication between IPv6-compatible terminals, techniques [1] and [2] are for sending IPv4 packets by encapsulating them in IPv6 packets in order to send them over sections of the network that are not compatible with IPv6.

Figure 3.4.1 shows an example of the tunneling configuration.

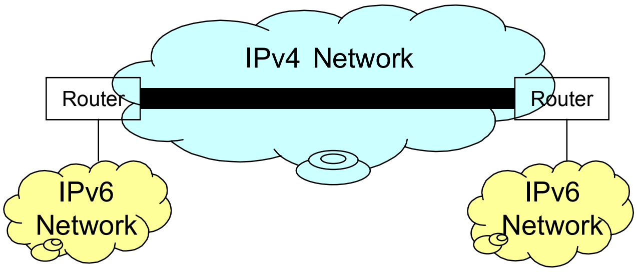


Figure 3.4.1: Example of Tunneling Configuration

(2) IPv4/IPv6 dual stack

Compatible with both IPv4 and IPv6 protocols, this is technique [2] for accessing the IPv6 server if the IPv6 address is known or using the IPv4 address to access the IPv4 server if the IPv6 address is not known. Internet Explorer is an example of this, but the user does not need to know whether it is IPv4 or IPv6. Figure 3.4.2 is an example of the IPv4/IPv6 dual stack operation.

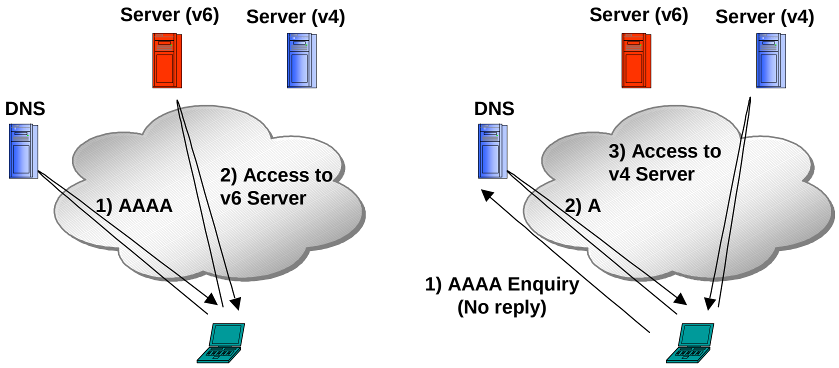


Figure 3.4.2: Example of IPv4/IPv6 Dual Stack Operation

(3) Multicast

IP multicast is a transmission system for efficient communication from one user to many users, which is able to reduce the load on the server and use network resources more efficiently than unicast transmission. This technique is not confined to IPv6 but in many cases it is not used in existing IPv4 networks, and the growing installation of IPv6 routers is expected to expedite its widespread use.

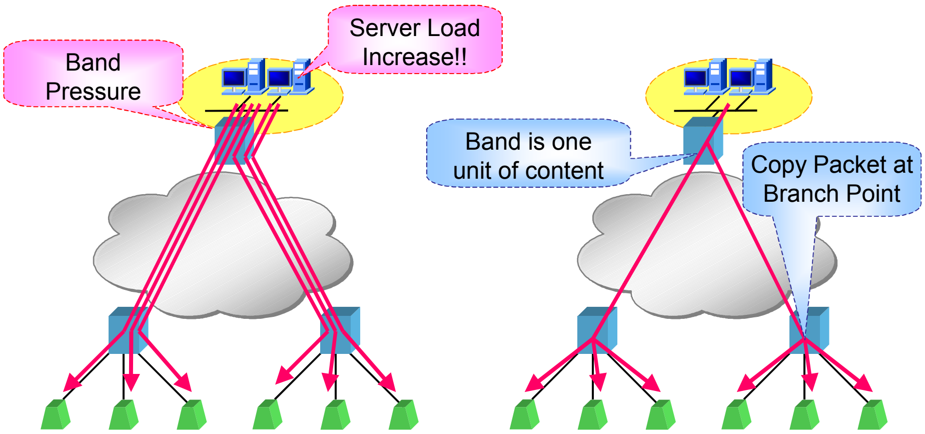


Figure 3.4.3: Unicast Transmission (Left) and Multicast Transmission (Right)

(4) Applications

At the application level, techniques for communication in a mixed IPv4/IPv6 environment are shown below.

(a) DNS server

By using standard applications, because they are compatible with the IPv4/IPv6 dual stack, IPv4 and IPv6 communications are both supported. Moreover, the names can be resolved with either the IPv4 protocol or the IPv6 protocol by adding “AAAA record” [4] to the zone file without changing the host name.

(b) Mail server

By using standard applications, because they are compatible with the IPv4/IPv6 dual stack, IPv4 and IPv6 communications are both supported.

(c) Web server

By using standard applications, because they are compatible with the IPv4/IPv6 dual stack, IPv4 and IPv6 communications are both supported.

(d) SIP translation

The SIP translation of the SIP-NAT server is technique [3] for SIP communication between IPv4 and IPv6 terminals, which is not compatible with the SIP server.

Figure 3.4.4 is an example of the SIP translation configuration.

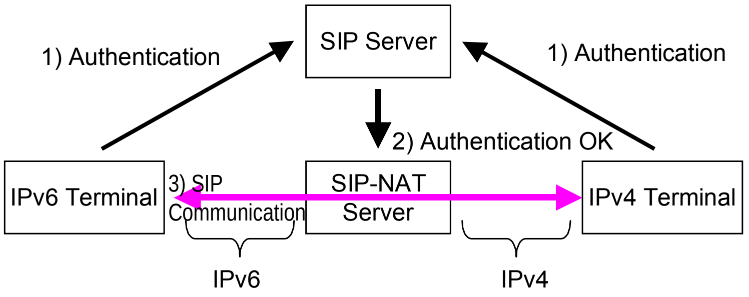


Figure 3.4.4: Example of SIP Translation Configuration

(e) Dual stack Web conferencing

The Web conference application sets up a communication server that is compatible with the IPv4/IPv6 dual stack. Moreover, a Web conference with a mixed environment of IPv4 terminals and IPv6 terminals is realized by providing for IPv4 usage and IPv6 usage on the terminal side module.

Figure 3.4.5 is an example of the Dual stack Web conferencing configuration.

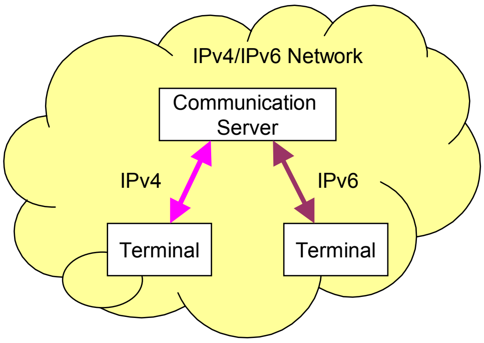


Figure 3.4.5: Example of Dual Stack Web Conferencing Configuration

(f) IPv4/IPv6 protocol conversion gateway

Even if the streaming control server (authentication server) is incompatible with the IPv4/IPv6 dual stack with respect to requests for authentication from IPv6 terminals, this is a technique for installing an IPv4/IPv6 protocol conversion gateway server to make the entire system compatible with the IPv4/IPv6 dual stack without altering the existing streaming control server (authentication server) application.

Figure 3.4.6 shows an example of an IPv4/IPv6 protocol conversion configuration

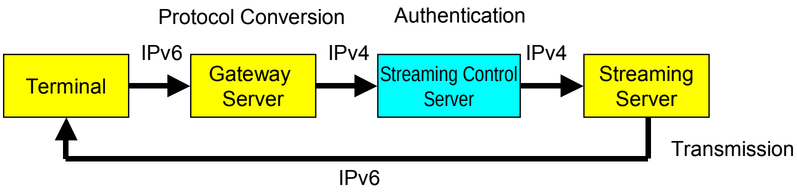


Figure 3.4.6: Example of IPv4/IPv6 Protocol Conversion Configuration

3.5 IPv6 Deployment Models

This deployment model is a concrete actualization of the relaxed model and the staged replacement type described in section 3.3, in accordance with the deployment model defined in section 3.2. In Part 2, evaluations are conducted by using the deployment model.

3.5.1 Present Configuration (Step 0)

The present configuration (Step 0) is the model of an environment with an IPv4 network only.

It is presupposed that the applications being used are SIP communication, a Web conference system, and video streaming. The Web conference system is configured with connections between terminals and the communication server by HTTP protocol. Video streaming works with each terminal by unicast. SIP communication is peer-to-peer communication through the server.

(1) Configuration

The present (Step 0) configuration is shown below.

(a) System configuration

Figure 3.5.1.1 shows the present (Step 0) verification configuration diagram.

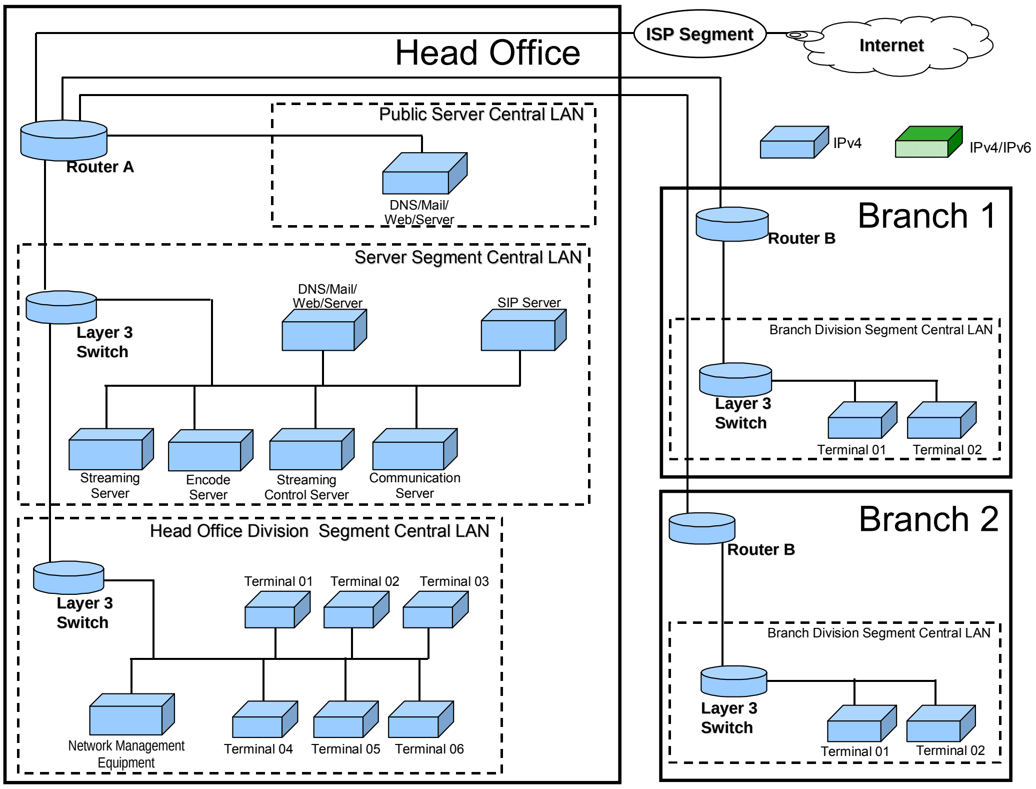


Figure 3.5.1.1: Diagram of Verification Configuration (Step 0)

Table 3.5.1.1 shows a table of component devices, each of which is explained below.

- Router A

  Router A is provided as the router for Internet connections and connections between branches and head office.

- Router B

  Router B is provided as the router for connecting the corporation's backbone network with divisional networks.

- Layer 3 switch

  Layer 3 switch is provided as a device for connecting the corporation's backbone network with divisional networks.

- Public DNS/Mail/Web servers

  Servers are established on the public server segment (DMZ) for making information available to the outside public. They act as relays for access from within the company to the outside.

- Internal DNS/Mail/Web servers
  Established in a server segment central LAN, all servers on the segment are registered on the DNS. Terminals in each division are to be registered in the DNS. Since the data is internal company information, access from outside is restricted.

- Streaming server
  Server for video stream transmission (on-demand and live).

- Encode server
  Live video input from cameras is MPEG-encoded and transmitted to the streaming server.

- Streaming control server
  For controlling (restricting number of accesses) data transmitted by the streaming server.

- Network management equipment
  Provides IPv4 network devices and servers for network management using SNMP.

- Communication server
  The communication server is provided as a server for conducting remote conferencing on the Web. Access with this server enables Web conference participants to share audio, animation and files.

- PC
  PCs using Windows XP are deployed as terminals for sharing video communication, the Web conferencing system, IP phone, and Web access.

Table 3.5.1.1: Basic Components of Verification Configuration (Step 0)

No.	Host name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	Router A (h-r01)	IX5020	Version 7.6.25	21	(ISP)	(ONU)	FastEther	
				22	b1-r01	E 0.0	Ethernet	
				23	b2-r01	E 0.0	Ethernet	
				24	h-sv01	fa	FastEther	
				26	h-r02	FE 0/1.0	FastEther	
				27	h-s01	11	FastEther	

2	Layer 3 switch (h-s01)	IX5003	Version 7.6.12	11	h-r01	27	FastEther	
				12	h-sv11	fa	FastEther	
					h-sv12	fa1	FastEther	
					h-sv13	fa1	FastEther	
					h-sv14	fa1	FastEther	
					h-sv15	fa1	FastEther	
					h-sv16	fa1	FastEther	
					h-sv17	fa1	FastEther	
					h-sv18	fa1	FastEther	
				13	h-s02	FE 0/1.0	FastEther	
3	Layer 3 switch (h-s02)	IX2010	Version 5.2.13	FE 0/0.0	h-s01	13	FastEther	
				FE 0/1.0	h-sv21	fa1	FastEther	
					h-cl01	fa	FastEther	
					h-cl02	fa	FastEther	
					h-cl03	fa	FastEther	
					h-cl04	fa	FastEther	
					h-cl05	fa	FastEther	
					h-cl06	fa	FastEther	
4	Router B (b1-r01)	IX1020	Version 5.2.13	E 0.0	h-r01	22	Ethernet	
				FE 0.0	b1-s01	FE 0/0.0	FastEther	
5	Layer 3 switch (b1-s01)	IX2010	Version 5.2.13	FE 0/0.0	b1-r01	FE 0.0	FastEther	
				FE 1/0.0	b1-cl01	fa	FastEther	
					b1-cl02	fa	FastEther	
6	Router B (b2-r01)	IX1020	Version 5.2.13	E 0.0	h-r01	23	Ethernet	
				FE 0.0	b2-s01	FE 0/0.0	FastEther	
7	Layer 3 switch (b2-s01)	IX2010	Version 5.2.13	FE 0/0.0	b2-r01	FE 0.0	FastEther	
				FE 1/0.0	b2-cl01	fa	FastEther	
					b2-cl02	fa	FastEther	
8	(h-r02)	IX2010	Version 5.2.13	FE 0/0.0	h-r01	24	FastEther	
				FE 0/1.0	h-r01	26	FastEther	
9	DNS/Mail/Web server (h-sv01)	LavieNX LW450	FreeBSD4.8	fa	h-r01	24	FastEther	
10	DNS/Mail/Web server (h-sv11)	LavieNX LW500	FreeBSD4.8	fa	h-s01	12	FastEther	
11	SIP server (h-sv13)	CX6820-SS	HP-UX 11i	fa	h-s01	12	FastEther	
12	Streaming server (h-sv14)	Express5800/ISS GS StreamPro	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
13	Encoder server (h-sv15)	Express5800/ISS ES	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
14	Streaming control server (h-sv16)	CX5000/F280R	Solaris9	fa1	h-s01	12	FastEther	
15	Communication server (h-sv17)	Express5800/120Rf-2	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
16	Network management equipment (h-sv21)	Express5800/110Rd-1	Windows Server 2003 Standard Edition	fa1	h-s02	FE 0/1.0	FastEther	
17	Head office terminal 01 (h-cl01)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
18	Head office terminal 02 (h-cl02)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
19	Head office terminal 03 (h-cl03)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
20	Head office terminal 04 (h-cl04)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
21	Head office terminal 05 (h-cl05)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
22	Head office terminal 06 (h-cl06)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
23	Branch office 1 terminal 01 (b1-cl01)	Versa Pro VY22X	Windows XP	fa	b1-s01	FE 1/0.0	FastEther	
24	Branch office 1 terminal 02 (b1-cl02)	Versa Pro VY22X	Windows XP	fa	b1-s01	FE 1/0.0	FastEther	
25	Branch office 2 terminal 01 (b2-cl01)	Versa Pro VY22X	Windows XP	fa	b2-s01	FE 1/0.0	FastEther	
26	Branch office 2 terminal 02 (b2-cl02)	Versa Pro VY22X	Windows XP	fa	b2-s01	FE 1/0.0	FastEther	

(b) Addresses

The private addresses that are used within a large enterprise are used for forming IPv4 addresses. Table 3.5.1.2 shows address designs.

Table 3.5.1.2: Verification Configuration (Step 0) Address Designs

Super Segment	Segment	Source			Network		Address	
		Host/Router	Phy. Port	Log. Port	IPv4	IPv6	IPv4	IPv6
Large enterprise network 192.0.2.32/28 2001:db8:2000::/48	Head office	Router A (h-r01)	21	VLAN1	192.0.2.40/30	-	192.0.2.42	-
			22	VLAN2	10.2.7.0 / 24	-	10.2.7.254	-
			23	VLAN3	10.2.8.0 / 24	-	10.2.8.254	-
			24	VLAN4	192.0.2.32 / 29	-	192.0.2.38	-
			25	VLAN8	-	-	-	-
			26	VLAN5	10.2.5.0 / 24	-	10.2.5.254	-
			27	VLAN6	10.2.6.0 / 24	-	10.2.6.254	-
			28	VLAN7	-	-	-	-
		Layer 3 switch (h-s01)	11	VLAN1	10.2.6.0 / 24	-	10.2.6.253	-
			12	VLAN2	10.2.10.0 / 24	-	10.2.10.254	-
			13	VLAN3	10.2.9.0 / 24	-	10.2.9.254	-
			14	-	-	-	-	-
			15	-	-	-	-	-
			16	-	-	-	-	-
			17	-	-	-	-	-
			18	-	-	-	-	-
		Layer 3 switch (h-s02)	FE 0/0.0	-	10.2.9.0 / 24	-	10.2.9.253	-
			FE 0/1.0	-	10.2.2.0 / 24	-	10.2.2.254	-
			FE 1/0.0	-	-	-	-	-
		(h-r02)	FE 0/0.0	-	192.0.2.32 / 29	-	192.0.2.37	-
			FE 0/1.0	-	10.2.5.0 / 24	-	10.2.5.253	-
			FE 1/0.0	-	-	-	-	-
	Branch 1	Router A (b1-r01)	E 0.0	-	10.2.7.0 / 24	-	10.2.7.253	-
			FE 0.0	-	10.2.1.0 / 24	-	10.2.1.254	-
		Layer 3 switch (b1-s01)	FE 0/0.0	-	10.2.1.0 / 24	-	10.2.1.253	-
			FE 0/1.0	-	-	-	-	-
			FE 1/0.0	-	10.2.3.0 / 24	-	10.2.3.254	-
	Branch 2	Router A (b2-r01)	E 0.0	-	10.2.8.0 / 24	-	10.2.8.253	-
			FE 0.0	-	10.2.11.0 / 24	-	10.2.11.254	-
		Layer 3 switch (b2-s01)	FE 0/0.0	-	10.2.11.0 / 24	-	10.2.11.253	-
			FE 0/1.0	-	-	-	-	-
			FE 1/0.0	-	10.2.4.0 / 24	-	10.2.4.254	-

(c) Routing

In a large enterprise network, the standard routing protocol OSPF is used for the conversion of path data between routers on the backbone network in the head office. RIP is used between head office and branch office and between branch line networks, which are at a comparatively small scale. Path data are imported mutually between OSPF and RIP, enabling routing over the entire large enterprise network. When necessary, path settings are also made with Static. Figure 3.5.1.2 shows the concept of routing in Step 0.

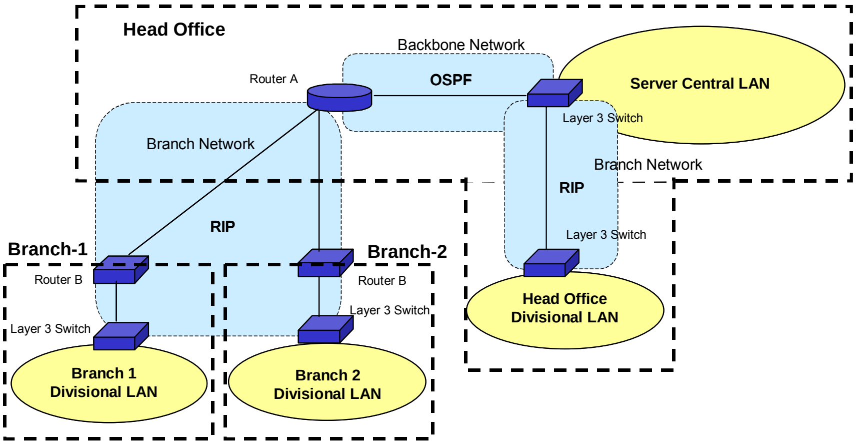


Figure 3.5.1.2: Conceptual Diagram of Routing (Step 0)

(d) Quality of Service (QoS) control

Traffic requiring real-time communication must be handled on network devices to give it priority over other traffic. Therefore, traffic related to Web conferencing and video streaming is given a QoS control setting that ensures preferential processing.

Table 3.5.1.3 shows assumed bands for each application used in Step 0.

Table 3.5.1.3: Assumed Bands Used by Each Application

Traffic type	Calculation standard	Assumed band	Notes
Video streaming	Unicast (MPEG-1)	1.5Mbps	
Web conferencing	30 [Kbps] × 5 [parties] × 2 [Group]	300kbps	Unicast

Now, in this deployment model, in any step, the highest priority voice traffic band was set to 1.5 Mbps. This was primarily because it is an adequate allocation for voice traffic and ensures a stable quality. Moreover, with a view to ensuring the maximum band in the physical band above 10 Mbps, a range that does not bring pressure on voice traffic, from past experience the band for motion picture traffic between head office and branches, which is the next highest priority, is given a QoS setting of 7 Mbps.

Table 3.5.1.4 shows the details of QoS settings.

Table 3.5.1.4: QoS Settings

No.	Target traffic	IPv4/IPv6	Conditions	Secured Band [Kbps]	QoS Class
1	Video streaming	IPv4	Source IP address = Streaming server	7000	af11
2		IPv4	Destination IP address = Streaming server		
3		IPv4	Source IP address = Streaming control server		
4		IPv4	Destination IP address = Streaming control server		
5	Web conferencing	IPv4	Source IP address = Communication server		
6		IPv4	Destination IP address = Communication server		

(e) Filter controls

Filter controls establish an interface on the Internet side of the backbone router (Router A) and allow access to the large enterprise network of only those packets that are received and that satisfy conditions for access permission. Table 3.5.1.5 shows details of the packet filters that have been established by this deployment model.

Table 3.5.1.5: Packet Filter Settings

No.	Conditions for access permission	IN/OUT
1	TCP communication by a completed TCP session	IN
2	UDP transmission source port number = 53 (DNS)	IN
3	TCP destination port number = 80 (http)	IN
4	TCP destination port number = 443 (https)	IN
5	TCP destination port number = 53 (DNS)	IN
6	UDP destination port number = 53 (DNS)	IN
7	TCP destination port number = 25 (SMTP)	IN
8	TCP destination port number = 22 (SSH)	IN
9	ICMP	IN

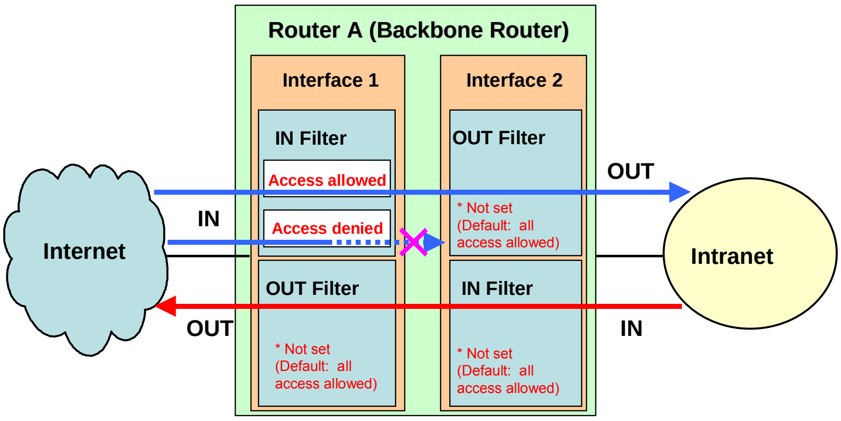


Figure 3.5.1.3: Filter Controls

3.5.2 Configuration of Migration Period (Step 1)

The migration period (Step 1) is a model that maintains continuity if there is partial migration to an IPv6 network environment and the rest remains in the existing IPv4 network environment.

For applications, we assume Internet telephony and Web conferencing using SIP as well as the use of video streaming.

Web conferencing will be connected in the same way as for Step 0 but the multi-address communication capability of IPv6 multicast will be used for transmitting shared data.

The capability of simultaneous reception of motion picture images to each terminal will be enabled by using IPv6 multicast for streaming other than Step 0 video stream transmission.

With this model, assuming the case in which there is an IPv4/IPv6 dual stack, and the Head office server segment central LAN and each divisional central LAN (Head office, Branch 1 and Branch 2) will take the lead over others, we are establishing a total of three IPv4-over-IPv6 tunnels to connect the Head office server segment central LAN with each divisional segment central LAN.

(1) Configuration

The configuration of migration period (Step 1) is shown below.

(a) System configuration

Figure 3.5.2.1 shows a diagram of the migration period (Step 1) verification configuration.

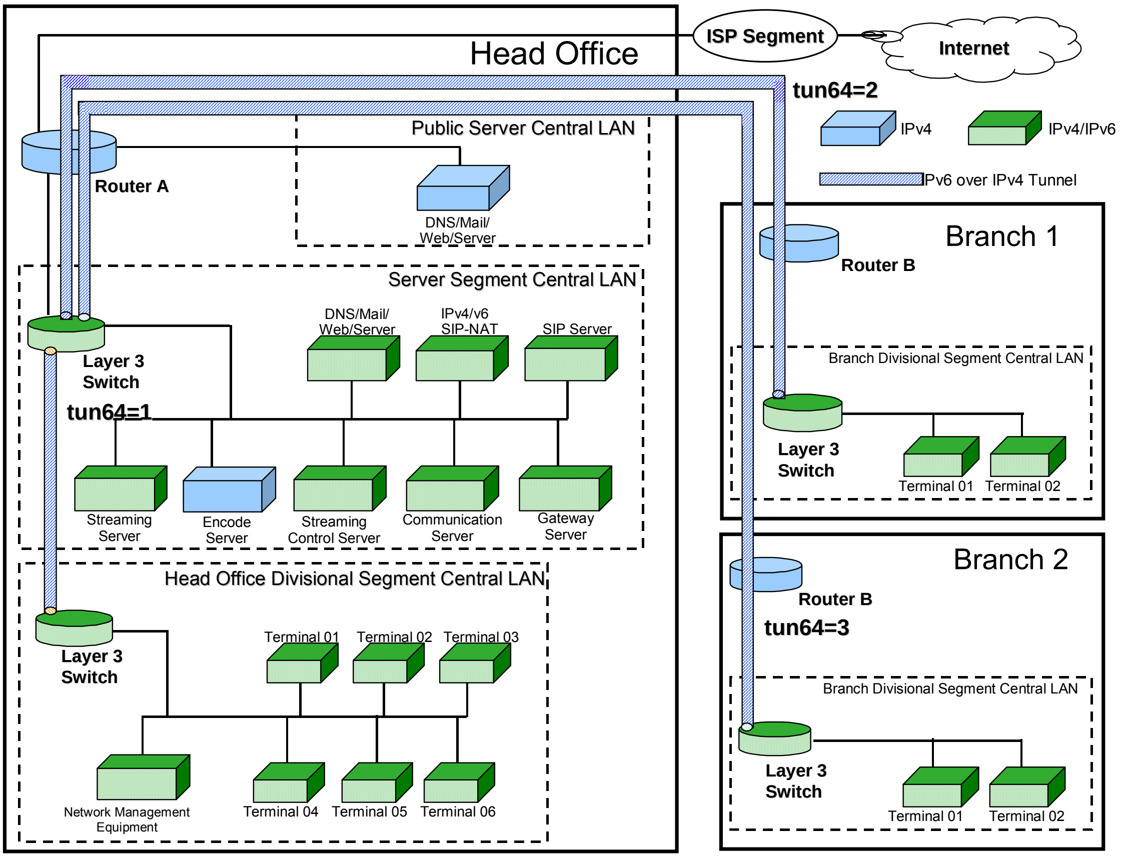


Figure 3.5.2.1: Diagram of Verification Configuration (Step 1)

Below, we explain the differences of devices from Step 0 in this empirical experiment and Table 3.5.2.1 shows the component devices.

- Layer 3 switches
  The addition of the IPv6 license has made this equipment compatible with IPv4/IPv6 dual stack.

- Public DNS/Mail/Web servers
  Adding an OS standard IPv6 protocol stack and various software version upgrades has made them compatible with the IPv4/IPv6 dual stack. The DNS server uses an IPv4/IPv6 dual stack compatible standard application, and we have added an IPv4/IPv6 dual stack compatible server's "AAAA record" [4] to the zone file.

- Internal DNS/Mail/Web servers
  Adding an OS standard IPv6 protocol stack and various software version upgrades has made them compatible with the IPv4/IPv6 dual stack. The DNS server uses an IPv4/IPv6 dual stack compatible standard application

and we have added an IPv4/IPv6 dual stack compatible server's "AAAA record" [4] to the zone file.

- Streaming server
  Adding an OS standard IPv6 protocol stack has made it compatible with the IPv4/IPv6 dual stack. IPv4/IPv6 dual stack compatible products are used for the applications.

- Network management equipment
  Adding an OS standard IPv6 protocol stack has made it compatible with the IPv4/IPv6 dual stack. IPv4/IPv6 dual stack compatible products are used for the applications.

- Communication server
  Adding an OS standard IPv6 protocol stack has made it compatible with the IPv4/IPv6 dual stack. IPv4/IPv6 dual stack compatible products are used for the applications.

- PC
  Adding an OS standard IPv6 protocol stack has made it compatible with the IPv4/IPv6 dual stack.

- Gateway server
  The gateway server, which converts IPv6 transmission requests into IPv4 transmission requests, is provided in order to request transmission to the existing IPv4 streaming control server when an IPv6 terminal receives a video transmission. The gateway server sends the transmission request by notifying the IPv6 address to the IPv6 terminal using the existing IPv4 streaming control system.

- IPv4/IPv6 SIP/NAT
  IPv4/IPv6 SIP/NAT is provided for the conversion of IPv4 addresses and IPv6 addresses in VoIP communication using the SIP protocol.

Table 3.5.2.1 Basic Components of Verification Configuration (Step 1)

No.	Host name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	Router A (h-r01)	IX5020	Version 7.6.25	21	(ISP)	(ONU)	FastEther	
				22	b1-r01	E 0.0	Ethernet	
				23	b2-r01	E 0.0	Ethernet	
				24	h-sv01	fa	FastEther	
				26	h-r02	FE 0/1.0	FastEther	
				27	h-s01	11	FastEther	
2	Layer 3 switch (h-s01)	IX5003	Version 7.6.12	11	h-r01	27	FastEther	
				12	h-sv11	fa	FastEther	
					h-sv12	fa1	FastEther	
					h-sv13	fa1	FastEther	
					h-sv14	fa1	FastEther	
					h-sv15	fa1	FastEther	
					h-sv16	fa1	FastEther	
					h-sv17	fa1	FastEther	
					h-sv18	fa1	FastEther	
				13	h-s02	FE 0/1.0	FastEther	
3	Layer 3 switch (h-s02)	IX2010	Version 5.2.13	FE 0/0.0	h-s01	13	FastEther	
				FE 0/1.0	h-sv21	fa1	FastEther	
					h-cl01	fa	FastEther	
					h-cl02	fa	FastEther	
					h-cl03	fa	FastEther	
					h-cl04	fa	FastEther	
					h-cl05	fa	FastEther	
					h-cl06	fa	FastEther	
4	Router B (b1-r01)	IX1020	Version 5.2.13	E 0.0	h-r01	22	Ethernet	
				FE 0.0	b1-s01	FE 0/0.0	FastEther	
5	Layer 3 switch (b1-s01)	IX2010	Version 5.2.13	FE 0/0.0	b1-r01	FE 0.0	FastEther	
				FE 1/0.0	b1-cl01	fa	FastEther	
					b1-cl02	fa	FastEther	
6	Router B (b2-r01)	IX1020	Version 5.2.13	E 0.0	h-r01	23	Ethernet	
				FE 0.0	b2-s01	FE 0/0.0	FastEther	
7	Layer 3 switch (b2-s01)	IX2010	Version 5.2.13	FE 0/0.0	b2-r01	FE 0.0	FastEther	
				FE 1/0.0	b2-cl01	fa	FastEther	
					b2-cl02	fa	FastEther	
8	(h-r02)	IX2010	Version 5.2.13	FE 0/0.0	h-r01	24	FastEther	
				FE 0/1.0	h-r01	26	FastEther	
9	DNS/Mail/Web Server (h-sv01)	LavieNX LW450	FreeBSD4.8	fa	h-r01	24	FastEther	
10	DNS/Mail/Web Server (h-sv11)	LavieNX LW500	FreeBSD4.8	fa	h-s01	12	FastEther	
11	IPv4/v6 SIP-NAT (h-sv12)	MX5840-NT	RedHat Linux 7.3	fa	h-s01	12	FastEther	
12	SIP Server (h-sv13)	CX6820-SS	HP-UX 11i	fa	h-s01	12	FastEther	
13	Streaming server (h-sv14)	Express5800/ISS GS StreamPro	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
14	Encode server (h-sv15)	Express5800/ISS ES	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
15	Streaming control server (h-sv16)	CX5000/F280R	Solaris9	fa1	h-s01	12	FastEther	
16	Communication server (h-sv17)	Express5800/120Rf-2	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
17	Gateway server (h-sv18)	Express5800/120Rf-2	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
18	Network management equipment (h-sv21)	Express5800/110Rd-1	Windows Server 2003 Standard Edition	fa1	h-s02	FE 0/1.0	FastEther	
19	Head office terminal 01 (h-cl01)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
20	Head office terminal 02 (h-cl02)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
21	Head office terminal 03 (h-cl03)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
22	Head office terminal 04 (h-cl04)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
23	Head office terminal 05 (h-cl05)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	

24	Head office terminal 06 (h-cl06)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
25	Branch 1 terminal 01 (b1-cl01)	Versa Pro VY22X	Windows XP	fa	b1-s01	FE 1/0.0	FastEther	
26	Branch 1 terminal 02 (b1-cl02)	Versa Pro VY22X	Windows XP	fa	b1-s01	FE 1/0.0	FastEther	
27	Branch 2 terminal 01 (b2-cl01)	Versa Pro VY22X	Windows XP	fa	b2-s01	FE 1/0.0	FastEther	
28	Branch 2 terminal 02 (b2-cl02)	Versa Pro VY22X	Windows XP	fa	b2-s01	FE 1/0.0	FastEther	

(b) Addresses

The address configuration in IPv4 uses private addresses similar to Step 0 and global addresses in IPv6.

Also, in the staged replacement type, even if each division adopts a dual stack, the whole address design must be established initially.

Table 3.5.2.2 shows address designs.

Table 3.5.2.2: Verification Configuration (Step 1) Address Designs

Super Segment	Segment	Source			Network		Address	
		Host/Router	Phy. Port	Log. Port	IPv4	IPv6	IPv4	IPv6
Large enterprise network 192.0.2.32/28 2001:db8:2000::/48	Head office	Router A (h-r01)	21	VLAN1	192.0.2.40/30	-	192.0.2.42	-
			22	VLAN2	10.2.7.0 / 24	-	10.2.7.254	-
			23	VLAN3	10.2.8.0 / 24	-	10.2.8.254	-
			24	VLAN4	192.0.2.32 / 29	-	192.0.2.38	-
			25	VLAN8	-	-	-	-
			26	VLAN5	10.2.5.0 / 24	-	10.2.5.254	-
			27	VLAN6	10.2.6.0 / 24	-	10.2.6.254	-
			28	VLAN7	-	-	-	-
		Layer 3 switch (h-s01)	11	VLAN1	10.2.6.0 / 24	-	10.2.6.253	-
				tun64-2	-	2001:db8:2000:5100:: / 64	-	2001:db8:2000:5100::1
				tun64-3	-	2001:db8:2000:5200:: / 64	-	2001:db8:2000:5200::1
			12	VLAN2	10.2.10.0 / 24	2001:db8:2000:1200:: / 64	10.2.10.254	2001:db8:2000:1200::1
			13	VLAN3	10.2.9.0 / 24	-	10.2.9.254	-
				tun64-1	-	2001:db8:2000:5000:: / 64	-	2001:db8:2000:5000::1
			14	-	-	-	-	-
			15	-	-	-	-	-
			16	-	-	-	-	-
			17	-	-	-	-	-
			18	-	-	-	-	-
		Layer 3 switch (h-s02)	FE 0/0.0	-	10.2.9.0 / 24	-	10.2.9.253	-
				tun0.0	-	2001:db8:2000:5000:: / 64	-	2001:db8:2000:5000::2
			FE 0/1.0	-	10.2.2.0 / 24	2001:db8:2000:1110:: / 64	10.2.2.254	2001:db8:2000:1110::1
			FE 1/0.0	-	-	-	-	-
		(h-r02)	FE 0/0.0	-	192.0.2.32 / 29	-	192.0.2.37	-
			FE 0/1.0	-	10.2.5.0 / 24	-	10.2.5.253	-
			FE 1/0.0	-	-	-	-	-
	Branch 1	Router A (b1-r01)	E 0.0	-	10.2.7.0 / 24	-	10.2.7.253	-
			FE 0.0	-	10.2.1.0 / 24	-	10.2.1.254	-
		Layer 3 switch (b1-s01)	FE 0/0.0	-	10.2.1.0 / 24	-	10.2.1.253	-
				tun0.0	-	2001:db8:2000:5100:: / 64	-	2001:db8:2000:5100::2
			FE 0/1.0	-	-	-	-	-
			FE 1/0.0	-	10.2.3.0 / 24	2001:db8:2000:3110:: / 64	10.2.3.254	2001:db8:2000:3110::1
	Branch 2	Router A (b2-r01)	E 0.0	-	10.2.8.0 / 24	-	10.2.8.253	-
			FE 0.0	-	10.2.11.0 / 24	-	10.2.11.254	-
		Layer 3 switch (b2-s01)	FE 0/0.0	-	10.2.11.0 / 24	-	10.2.11.253	-
				tun0.0	-	2001:db8:2000:5200:: / 64	-	2001:db8:2000:5200::2
			FE 0/1.0	-	-	-	-	-
			FE 1/0.0	-	10.2.4.0 / 24	2001:db8:2000:2110:: / 64	10.2.4.254	2001:db8:2000:2110::1

(c) Routing

In IPv4, path data is similar to that for Step 0. For IPv6, RIPng is used only for communication between divisional and branch networks. Also, path settings can be partially static.

Figure 3.5.2.2 shows the concept of routing in Step 1.

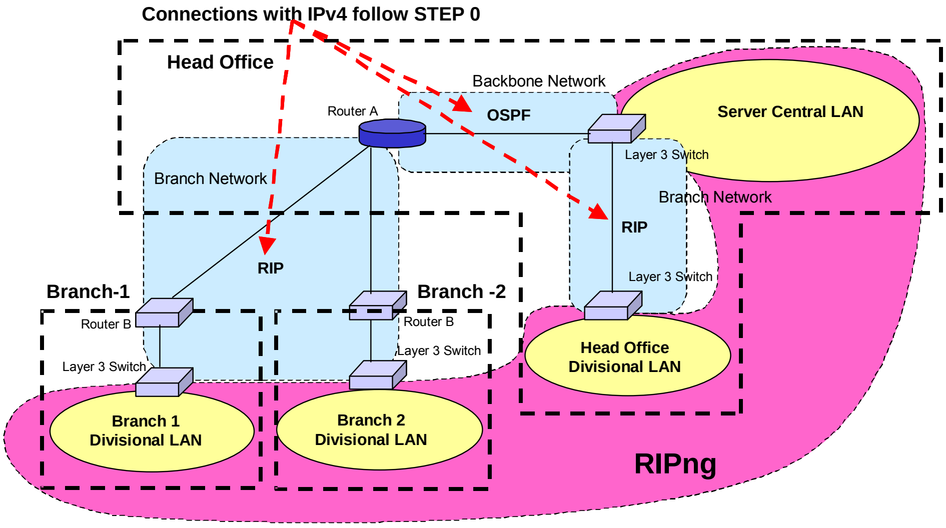


Figure 3.5.2.2: Conceptual Diagram of Routing (Step 1)

(d) Multicast

i) Summary

The multi-address communication capability of IPv6 multicast will be used for transmitting common video streaming and Web conferencing data. This not only ensures simultaneous reception capability at each terminal but also reduces the load on the network.

ii) Multicast group addresses

IPv6 multicast addresses begin with a FF header. If the next four bits are zeroes, this indicates a permanent address, and if they are ones, this indicates a temporary address. The next following four bits designate the multicast target scope. The main scopes include “2:Link-Local”, “5:Site-Local”, “8:Organization-Local” and “e:Global”. For example, using “ff15::1" with Site-Local would indicate a temporary multicast address. In Step 1, “8:Organization-Local” is selected.

Table 3.5.2.3 shows the multicast group addresses used in Step 1

Table 3.5.2.3: IPv6 Multicast Group Addresses

No.	Application	Multicast Group Address	Notes
1	Video streaming	ff18::1	
2	Web conferencing	ff18::1:*	* optional value

iii) Multicast routing

PIM-SM [5] is used for multicast routing with the router that accommodates the servers, and MLD-proxy is used for multicast routing between IPv6 islands. Since the rendezvous point (RP) to be used by the PIM-SM must be set as the router at the center of the streaming tree structure, for this configuration, it is set at the head office layer 3 switch that accommodates the servers. Moreover, the bootstrap router (BSR) that transmits the bootstrap message must be set to the lowest candidate within the multicast domain, and this is also set to the head office layer 3 switch. The reason for setting the layer 3 switch as the RP and BSR candidate is that the multicast streaming server is connected there and the layer 3 switch is supposed to behave normally.

Figure 3.5.2.3 shows the specified position of the RP and BSR.

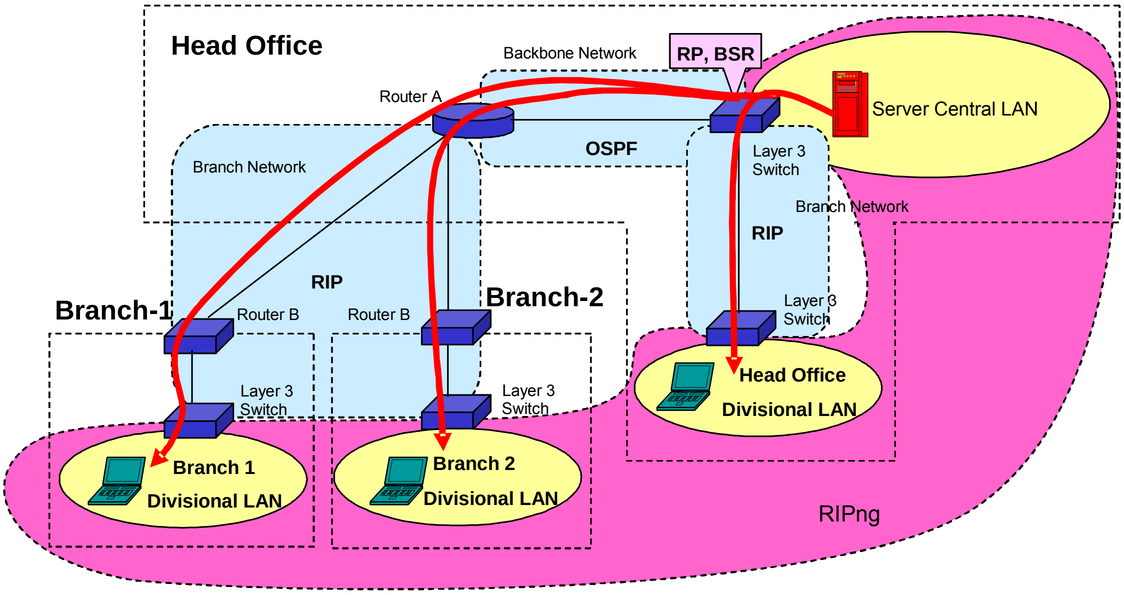


Figure 3.5.2.3: Specified Position of the RP and BSR

(e) QoS Control

For IPv4 traffic, it is similar to Step 0. For IPv6 traffic, QoS control settings are added to IPv4-over-IPv6 tunneling. Table 3.5.2.4 shows details of QoS control settings.

In addition, Table 3.5.2.5 shows the assumed bands for each application used in Step 1.

Table 3.5.2.4: QoS Settings

No.	Target Traffic	IPv4/IPv6	Conditions	Secured Band [Kbps]	QoS Class
1	Video streaming	IPv4	Source IP address = Streaming server	7000	af11
2		IPv4	Destination IP address = Streaming server		
3		IPv4	Source IP address = Streaming control server		
4		IPv4	Destination IP address = Streaming control server		
5	Web conferencing	IPv4	Source IP address = Communication server		
6		IPv4	Destination IP address = Communication server		
7	Web conferencing	IPv4	Source IP address = IP tunnel entry	1500	ef2
8		IPv4	Destination IP address = IP tunnel exit		

Table 3.5.2.5: Assumed Bands Used by Each Application

Traffic Type	Calculation standard	Assumed band	Notes
SIP telephony	16 [Kbps]×10 [lines]	160kbps	
Web conferencing	30 [Kbps] × 5 [parties] × 2 [groups]	300kbps	Unicast
	100 [Kbps] × 5 [parties] × 1 [group]	500kbps	Multicast
Video streaming	Unicast (MPEG-1)	1.5Mbps	
	Multicast (MPEG-1)	1.5Mbps	
	Multicast (MPEG-2)	4Mbps	

(f) Filter controls

The filter establishes an interface on the Internet side of the backbone router and allows access into the large enterprise network of only those packets that are received and that satisfy conditions for access permission. Details of the packet filter that has been established for this deployment model are the same as for Step 0.

(2) Migration procedure

The procedure for migration from the IPv4 environment of Step 0 to the IPv4/IPv6 environment of Step 1 is given below.

(a) Adjustment of conditions

Problem areas such as routers or other devices along the path through an IPv6 tunnel of an IPv6 island that had a connection request in IPv6, or problems concerning applications to be used in the IPv6 tunnel environment, need to be sorted out.

(b) Network design

Make specific designs such as routers for the sections that pass IPv6 tunnels in the entire company network on the basis of problems that have arisen in the adjustment of conditions.

(c) Config settings

On the basis of the network design document, design configs for such devices as the routers and layer 3 switches that establish IPv6-over-IPv4 tunnels.

(d) Daily schedule planning

Notify the end user beforehand about interrupted sections of the network and time zones by making adjustments to daily schedules for changing settings for routers, layer 3 switches, and other devices.

(e) Network-related settings and verification

The configs that were created beforehand are to be set with respect to the relevant devices. However, since there may be some cases such as router resetting when the settings are made, the sequence in which devices are to be set must be taken into account.

Following are some specific tasks that were performed during the empirical experiments:

- Switch on the configs that were created beforehand with the server segment layer 3 switches and divisional LAN layer 3 switches.
- Set each server so that the various IPv6 compatible applications become IPv4/IPv6 dual stack compatible (including IPv4/IPv6 SIP-NAT and gateway server settings).

For the network devices that have been set, confirm mutual communication and verify performance in IPv4 and IPv6.

(f) Terminal settings

Install an IPv6 stack at each terminal to make it IPv4/IPv6 dual stack compatible.

(g) Confirmation of action

Confirm that IPv6 communication for the various applications is proceeding from each terminal.

(3) Important notices

(a) Address assignments

IPv6 addresses normally have a /48 address prefix assigned by the ISP, but since a

/64 subnet can assign 65,000 items, we can say this is enough for normal usage. In this step, it would be preferable to have a legitimate global address when an IPv6 address is first assigned, but here, since there will not be any Internet connection, we could also make a temporary address. However, considering a future Internet connection, it is probably better to define the subnet and systematize it by obtaining a /48 address prefix. Concerning the assignment of temporary addresses, the IPv6 Deployment Working Group is debating methods of applying rules for the creation of global IPv4 and IPv6 addresses.

(b) Maximum transmission unit (MTU) size

If an IPv6-over-IPv4 tunnel is to be used, a 20-byte header is added in order to encapsulate an IPv6 packet in an IPv4 packet. Consequently, if a packet that is to be transmitted is the full MTU size of the receiving network and this is the same as the MTU size of the destination network, the packet will be divided and transmitted by the router. This action is called fragmenting and may become a cause of reduced router performance. In order to prevent this, IPv6 is so arranged that in accordance with an ICMPv6 “Packet too big” message, the transmitting host will transmit within the end-to-end MTU size.

However, ICMPv6 packets may not necessarily function well because, for purposes such as preventing DOS attack, they may be disallowed transmission over the network and discarded by the host. Therefore, actually, there may be cases where fragmenting by the router is unavoidable, and as a result, the performance of the network cannot be fully realized and packet loss may occur. This may be particularly prominent especially when wide-area multimedia applications are being used.

The problem mentioned above was fully considered in the implementation of Router A used in this verification and the layer 3 switches that accommodate the server groups. That is to say, fast hardware transmission will continue even if fragmenting should occur in sending a packet to a tunnel interface and there was no particular trouble even with MPEG2 IP multicast transmission (4 Mbps).

In other words, in a case of introducing a wide-area multimedia application, equipment that is capable of handling fragmenting must be selected or the streaming server’s MTU must be set specifically.

(c) Multicast traffic

QoS settings have been established for bandwidth control of IPv6 multimedia applications, but peak rates at that time are nearly twice the encoder bandwidth. This is due to traffic bursts and variations within the network caused by high bandwidth streaming transmissions that consume the network bandwidth momentarily. In empirical experiments, combined with traffic characteristics that depend on the server, this corresponded to minimum values obtained by cut-and-try QoS settings of the router that would prevent discard.

Since the processing of IPv6 traffic in a tunnel by finely discriminating control in the backbone network becomes complicated, it was established as the total traffic of an IPv6-over-IPv4 tunnel. This was because we judged that, as it was the first stage of deploying IPv6, not much traffic would be generated and also there would be little effect on the existing IPv4 traffic.

3.5.3 Configuration of Migration Period (Step 2)

The migration period (Step 2) is a model that takes account of connectivity with existing IPv4 terminals by the whole network environment, including the backbone network of the large enterprise, migrating to an IPv6 network. The network environment, including networks within divisions as well as the backbone network, is constructed under IPv4/IPv6 dual stack. This enables the time for processing IPv4 header parts by router to be shortened by dismantling the IPv6-over-IPv4 tunnel that was established in Step 1. This will also enable the network to be used more efficiently if there should be an increase in divisions. Applications presuppose the use of Internet telephony using SIP, Web conferencing, and streaming transmission.

(1) Configuration

The configuration of the migration period (Step 2) is shown below.

(a) System configuration

Figure 3.5.3.1 shows a verification configuration diagram of the migration period (Step 2).

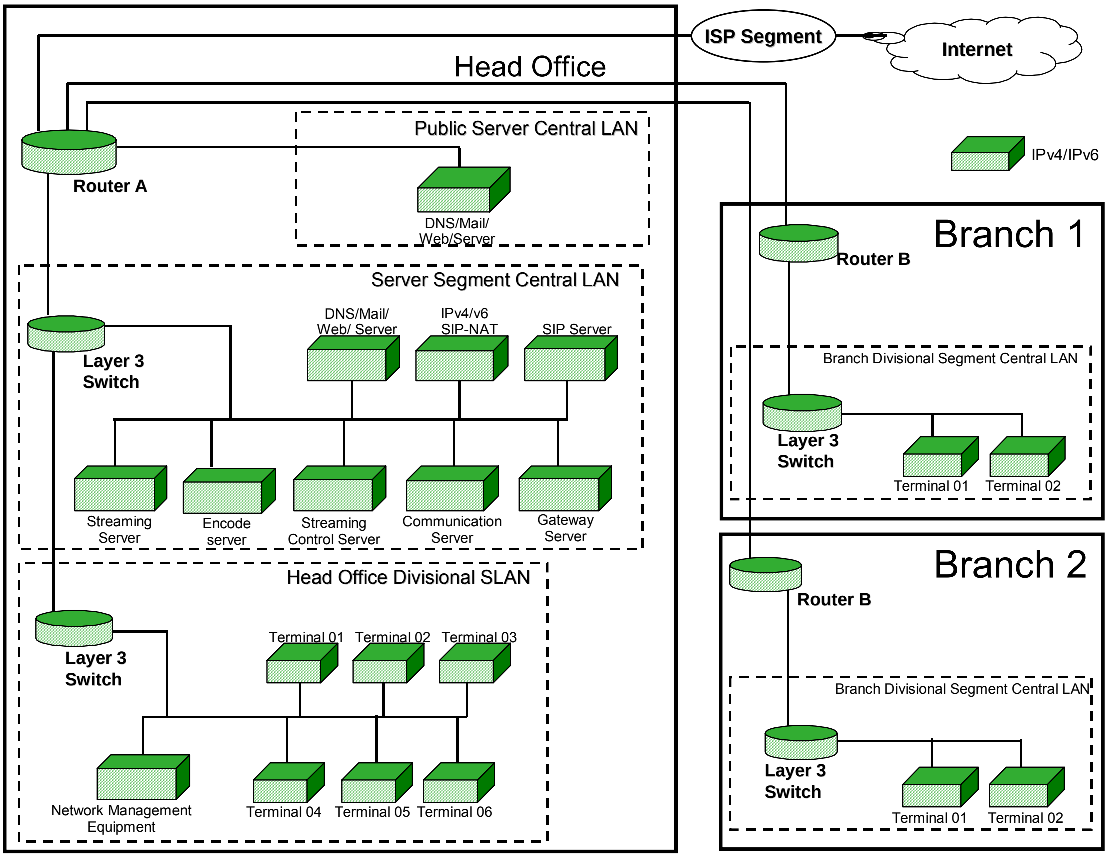


Figure 3.5.3.1: Diagram of Verification Configuration (Step 2)

Differences in devices from Step 1 in these empirical experiments are explained below, and Table 3.5.3.1 shows component devices.

- Router A

  The addition of an IPv6 license for this equipment has made it compatible with IPv4/IPv6 dual stack.

- Router B

  The addition of an IPv6 license for this equipment has made it compatible with IPv4/IPv6 dual stack.

Table 3.5.3.1: Basic Components of Verification Configuration (Step 2)

No.	Host name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	Router A (h-r01)	IX5020	Version 7.6.25	21	(ISP)	(ONU)	FastEther	
				22	b1-r01	E 0.0	Ethernet	
				23	b2-r01	E 0.0	Ethernet	
				24	h-sv01	fa	FastEther	
				26	h-r02	FE 0/1.0	FastEther	
				27	h-s01	11	FastEther	
2	Layer 3 switch　(h-s01)	IX5003	Version 7.6.12	11	h-r01	27	FastEther	
				12	h-sv11	fa	FastEther	
					h-sv12	fa1	FastEther	
					h-sv13	fa1	FastEther	
					h-sv14	fa1	FastEther	
					h-sv15	fa1	FastEther	
					h-sv16	fa1	FastEther	
					h-sv17	fa1	FastEther	
					h-sv18	fa1	FastEther	
				13	h-s02	FE 0/1.0	FastEther	
3	Layer 3 switch　(h-s02)	IX2010	Version 5.2.13	FE 0/0.0	h-s01	13	FastEther	
				FE 0/1.0	h-sv21	fa1	FastEther	
					h-cl01	fa	FastEther	
					h-cl02	fa	FastEther	
					h-cl03	fa	FastEther	
					h-cl04	fa	FastEther	
					h-cl05	fa	FastEther	
					h-cl06	fa	FastEther	
4	Router B (b1-r01)	IX1020	Version 5.2.13	E 0.0	h-r01	22	Ethernet	
				FE 0.0	b1-s01	FE 0/0.0	FastEther	
5	Layer 3 switch　(b1-s01)	IX2010	Version 5.2.13	FE 0/0.0	b1-r01	FE 0.0	FastEther	
				FE 1/0.0	b1-cl01	fa	FastEther	
					b1-cl02	fa	FastEther	
6	Router B (b2-r01)	IX1020	Version 5.2.13	E 0.0	h-r01	23	Ethernet	
				FE 0.0	b2-s01	FE 0/0.0	FastEther	
7	Layer 3 switch　(b2-s01)	IX2010	Version 5.2.13	FE 0/0.0	b2-r01	FE 0.0	FastEther	
				FE 1/0.0	b2-cl01	fa	FastEther	
					b2-cl02	fa	FastEther	
8	(h-r02)	IX2010	Version 5.2.13	FE 0/0.0	h-r01	24	FastEther	
				FE 0/1.0	h-r01	26	FastEther	
9	DNS/Mail/Web Server (h-sv01)	LavieNX LW450	FreeBSD4.8	fa	h-r01	24	FastEther	
10	DNS/Mail/Web Server (h-sv11)	LavieNX LW500	FreeBSD4.8	fa	h-s01	12	FastEther	
11	IPv4/v6 SIP-NAT (h-sv12)	MX5840-NT	RedHat Linux 7.3	fa	h-s01	12	FastEther	
12	SIP Server (h-sv13)	CX6820-SS	HP-UX 11i	fa	h-s01	12	FastEther	
13	Streaming Server (h-sv14)	Express5800/ISS GS StreamPro	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
14	Encode server (h-sv15)	Express5800/ISS ES	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
15	Streaming control Server (h-sv16)	CX5000/F280R	Solaris9	fa1	h-s01	12	FastEther	
16	Communication Server (h-sv17)	Express5800/120Rf-2	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
17	Gateway Server (h-sv18)	Express5800/120Rf-2	Windows Server 2003 Standard Edition	fa1	h-s01	12	FastEther	
18	Network management equipment (h-sv21)	Express5800/110Rd-1	Windows Server 2003 Standard Edition	fa1	h-s02	FE 0/1.0	FastEther	
19	Head office terminal 01 (h-cl01)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
20	Head office terminal 02 (h-cl02)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
21	Head office terminal 03 (h-cl03)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
22	Head office terminal 04 (h-cl04)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
23	Head office terminal 05 (h-cl05)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	
24	Head office terminal 06 (h-cl06)	Versa Pro VY22X	Windows XP	fa	h-s02	FE 0/1.0	FastEther	

25	Branch 1 terminal 01 (b1-cl01)	Versa Pro VY22X	Windows XP	fa	b1-s01	FE 1/0.0	FastEther	
26	Branch 1 terminal 02 (b1-cl02)	Versa Pro VY22X	Windows XP	fa	b1-s01	FE 1/0.0	FastEther	
27	Branch 2 terminal 01 (b2-cl01)	Versa Pro VY22X	Windows XP	fa	b2-s01	FE 1/0.0	FastEther	
28	Branch 2 terminal 02 (b2-cl02)	Versa Pro VY22X	Windows XP	fa	b2-s01	FE 1/0.0	FastEther	

(b) Addresses

Address configuration is similar to Step 1, private addresses in IPv4 and global addresses in IPv6.

Table 3.5.3.2 shows address designs.

Table 3.5.3.2: Verification Configuration (Step 2) Address Designs

Super Segment	Segment	Source			Network		Address	
		Host/Router	Phy. Port	Log. Port	IPv4	IPv6	IPv4	IPv6
Large enterprise network 192.0.2.32/28 2001:db8:2000::/48	Head office	Router A (h-r01)	21	VLAN1	192.0.2.40/30	-	192.0.2.42	-
			22	VLAN2	10.2.7.0 / 24	2001:db8:2000:3000:: / 64	10.2.7.254	2001:db8:2000:3000::1
			23	VLAN3	10.2.8.0 / 24	2001:db8:2000:2000:: / 64	10.2.8.254	2001:db8:2000:2000::1
			24	VLAN4	192.0.2.32 / 29	-	192.0.2.38	-
			25	VLAN8	-	2001:db8:2000:4000:: / 64	-	2001:db8:2000:4000::1
			26	VLAN5	10.2.5.0 / 24	-	10.2.5.254	-
			27	VLAN6	10.2.6.0 / 24	2001:db8:2000:1000:: / 64	10.2.6.254	2001:db8:2000:1000::1
			28	VLAN7	-	2001:218:2140:101:: / 64	-	2001:218:2140:101::2
		Layer 3 switch (h-s01)	11	VLAN1	10.2.6.0 / 24	2001:db8:2000:1000:: / 64	10.2.6.253	2001:db8:2000:1000::2
			12	VLAN2	10.2.10.0 / 24	2001:db8:2000:1200:: / 64	10.2.10.254	2001:db8:2000:1200::1
			13	VLAN3	10.2.9.0 / 24	2001:db8:2000:1100:: / 64	10.2.9.254	2001:db8:2000:1100::1
			14	-	-	-	-	-
			15	-	-	-	-	-
			16	-	-	-	-	-
			17	-	-	-	-	-
			18	-	-	-	-	-
		Layer 3 switch (h-s02)	FE 0/0.0	-	10.2.9.0 / 24	2001:db8:2000:1100:: / 64	10.2.9.253	2001:db8:2000:1100::2
			FE 0/1.0	-	10.2.2.0 / 24	2001:db8:2000:1110:: / 64	10.2.2.254	2001:db8:2000:1110::1
			FE 1/0.0	-	-	-	-	-
		(h-r02)	FE 0/0.0	-	192.0.2.32 / 29	-	192.0.2.37	-
			FE 0/1.0	-	10.2.5.0 / 24	-	10.2.5.253	-
			FE 1/0.0	-	-	-	-	-
	Brancfh 1	Router A (b1-r01)	E 0.0	-	10.2.7.0 / 24	2001:db8:2000:3000:: / 64	10.2.7.253	2001:db8:2000:3000::2
			FE 0.0	-	10.2.1.0 / 24	2001:db8:2000:3100:: / 64	10.2.1.254	2001:db8:2000:3100::1
		Layer 3 switch (b1-s01)	FE 0/0.0	-	10.2.1.0 / 24	2001:db8:2000:3100:: / 64	10.2.1.253	2001:db8:2000:3100::2
			FE 0/1.0	-	-	-	-	-
			FE 1/0.0	-	10.2.3.0 / 24	2001:db8:2000:3110:: / 64	10.2.3.254	2001:db8:2000:3110::1
	Brancfh 2	Router A (b2-r01)	E 0.0	-	10.2.8.0 / 24	2001:db8:2000:2000:: / 64	10.2.8.253	2001:db8:2000:2000::2
			FE 0.0	-	10.2.11.0 / 24	2001:db8:2000:2100:: / 64	10.2.11.254	2001:db8:2000:2100::1
		Layer 3 switch (b2-s01)	FE 0/0.0	-	10.2.11.0 / 24	2001:db8:2000:2100:: / 64	10.2.11.253	2001:db8:2000:2100::2
			FE 0/1.0	-	-	-	-	-
			FE 1/0.0	-	10.2.4.0 / 24	2001:db8:2000:2110:: / 64	10.2.4.254	2001:db8:2000:2110::1

(c) Routing

In IPv4, path data is similar to that for Step 0. For IPv6 also, OSPF is used for the conversion of path data between head office backbone network routers. RIPng is used between head office and branches and between divisional and branch networks. Path data is imported mutually between OSPF and RIPng, enabling routing on the large enterprise network as a whole. Also, static path settings are made as required.

Figure 3.5.3.2 shows the concept of routing in Step 2.

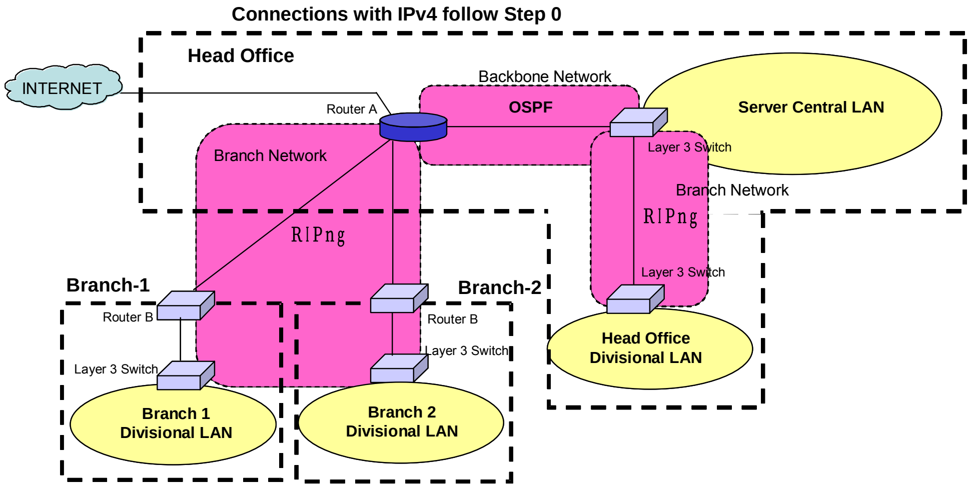


Figure 3.5.3.2: Conceptual Diagram of Routing (Step 2)

(d) Multicast

Multicast settings in Step 2 (group addresses, routing, etc.) are similar to Step 1. Differences from Step 1 include the disappearance of the IPv6-over-IPv4 tunnel, which means there is a different multicast allocation interface and a different MLD-proxy allocation interface.

Priorities can be established for RP and BSR mentioned in Step 1. In Step 2, these priority settings are applied in order to add new IPv6 multicast communication with the Internet. By setting a high priority for communication within the intranet and a low priority for communication with the Internet, the internal RP is selected preferentially when communication is within the intranet, and the external RP is selected when communication is with the Internet.

(e) QoS control

For IPv4 traffic, this is the same as Step 0.

For SIP telephony, because of the need for the maximum real-time activity, the most preferential (ef1) setting for all IPv4 and IPv6 is established. For Web conferencing and video streaming traffic (whether IPv4/IPv6 or Multicast/Unicast), the next most preferential setting after SIP telephony (af11) is established. Even with the same application, separate bands are allocated for IPv4 and IPv6, but since an increase in IPv6 traffic means a migration from IPv4, when the total of IPv4 and IPv6 is viewed, the traffic can be about the same.

Table 3.5.3.3 shows details of QoS settings in Step 2.

Also, Table 3.5.3.4 shows assumed bandwidths for each application in Step 2.

Table 3.5.3.3: QoS Settings

No.	Target Traffic	IPv4/IPv6	Separation Conditions	Secured band [Kbps]	QoS Class
1	Video Streaming	IPv4	Source IP address = Streaming server	7000	af11
2		IPv4	Destination IP address = Streaming server		
3		IPv4	Source IP address = Streaming control server		
4		IPv4	Destination IP address = Streaming control server		
5	Web Conferencing	IPv4	Source IP address = Communication server		
6		IPv4	Destination IP address = Communication server		
7	SIP Telephony	IPv6	Source port number = SIP client usage port range	1500	ef1
8		IPv6	Destination port number = SIP client usage port range		
9		IPv6	Source IP address = SIP server		
10		IPv6	Destination IP address = SIP server		
11	Video Streaming	IPv6	Source IP address = Streaming server	7000	af11
12		IPv6	Destination IP address = Streaming server		
13		IPv6	Source IP address = Streaming control server		
14		IPv6	Destination IP address = Streaming control server		
15	Web Conferencing	IPv6	Source IP address = Communication server		
16		IPv6	Destination IP address = Communication server		
17	Video Streaming （Multicast）	IPv6	Destination IP address = Multicast group address for stream transmission		
18	Web Conferencing （Multicast）	IPv6	Destination IP address = Multicast group address for Web conferencing		

Table 3.5.3.4: Assumed Bandwidths Used for Each Application

Traffic Type	Calculation standard	Assumed band	Notes
SIP telephony	16 [Kbps]×10 [lines]	160kbps	
Web conferencing	30 [Kbps] × 5 [parties] × 2 [groups]	300kbps	Unicast
	100 [Kbps] × 5 [parties] × 1 [group]	500kbps	Multicast
Video streaming	Unicast (MPEG-1)	1.5Mbps	
	Multicast (MPEG-1)	1.5Mbps	
	Multicast (MPEG-2)	4Mbps	

(f) Filter controls

The filter establishes an interface on the Internet side of the backbone router and allows access into the large enterprise network of only those packets that are received and that satisfy conditions for access permission. Details of the packet filter that has been established for this deployment model are the same as for Step 0.

(2) Migration procedure

The procedure for migration from the IPv4/IPv6 tunneling environment of Step 1 to the IPv4/IPv6 dual stack environment of Step 2 is given below.

(a) Adjustment of conditions

Sort out problems and other issues concerning the network equipment and applications to be used in the IPv4/IPv6 dual stack environment when the whole company network migrates to the IPv4/IPv6 dual stack environment.

(b) Network design

Make specific designs for when the whole network is under an IPv4/IPv6 dual stack environment over the entire company network on the basis of problems that have arisen in the adjustment of conditions.

(c) Config design

Design configs for each device under IPv4/IPv6 dual stack (routers, layer 3 switches, etc.) based on the network design document.

(d) Daily schedule planning

Coordinate with each division to make a daily schedule plan for changing settings for the routers, layer 3 switches, and other devices. Notify end users beforehand about interrupted sections of the network and timeframes based on the daily schedule plan.

(e) Network-related settings and verification

The configs that were created beforehand are to be set with respect to the relevant devices on the basis of the daily schedule plan. However, since there may be some cases such as router resetting when the settings are made, the sequence in which devices are to be set must be taken into account.

The following are some specific tasks that were performed during the empirical experiments:

- Switch on the configs that were created beforehand to the devices that constitute the backbone network (Router A, Router B, and server segment layer 3 switches).
- Set each server so that the various IPv6 compatible applications become IPv4/IPv6 dual stack compatible (including SIP-NAT and gateway server settings).
- For the network devices that have been set, confirm mutual communication and verify performance in IPv4 and IPv6.
- Switch on the configs that were created beforehand to layer 3 switches for branches, etc. Remove IPv6-over-IPv4 tunnels that were set for branches and other areas in Step 1.
- For the network devices that have been set, confirm mutual communication and verify performance in IPv4 and IPv6.
- Proceed to implement the switchover of each division in sequence.

(f) Setting terminals

Install IPv6 stacks in the various terminals other than divisional terminals that were already made IPv4/IPv4 dual stack compatible in Step 1.

(g) Confirm operation

Use IPv6 communication from each terminal to confirm operation for the various applications.

(3) Important notices

(a) Address assignment

For IPv6 connection to the Internet, at least a valid IPv6 address must be acquired at this time. This will also mean reassigning the IPv6 addresses of the intranet's internal routers.

If the /48 address assignment policy that was established in Step 1 is followed, changing the router settings required for this should not be too difficult a task, as only the higher prefix needs to be changed. Moreover, it might also be advantageous to take this opportunity to change to an address assignment suitable for the form of organization at that time.

(b) Firewall

For Internet connections in a large enterprise, it is customary to install a firewall to ensure uniform security. Because no firewall product had been released that is able to cope with multimedia traffic including IP multicast, we opted to cope by means of a router filter function.

This enabled the use of high-performance hardware transmission for connecting IP multicast to the Internet. Problems to be solved include the inability to collect an access log and lack of detailed control such as stateful access control.

(c) Multicast

In the empirical experiments, the multicast connection was also set to enable the reception of transmissions from the Internet. Here, from the aspect of preventing the leakage of information, access to the company's internal multicast transmissions from outside should be disabled. However, a firewall product that has this function has not been released at this time.

In this regard, in these empirical experiments, by using a fixed RP for the company's internal multicast group (organization local scope), any request from outside for transmission is actually disabled by the routing level without transmitting the RP candidates to the external PIM-SM router. Another conceivable method would be to establish a filter for the IP multicast data itself, but this might generate traffic that is useless to part of the network, which cannot be said to be satisfactory from the aspect of efficient use of network resources.

If a transmission outside the company is to be made, this can be done by using a global scope multicast group.

3.6 Evaluations and Observations

In this section, we evaluate and offer some thoughts on the results obtained from the concrete migration work described in section 3.5. We present these evaluations and thoughts on deployment procedures from the viewpoints of the constructor, the operator, and the user.

3.6.1 From the Viewpoint of the Constructor

The constructor must consider whether the services that can be realized by IPv6 and which are demanded by the user can be deployed reliably and efficiently.

(1) Network migration

Concerning the deployment of IPv6, compatibility of routers and switches can be achieved in many cases by firmware upgrades and the addition of a license. This helps to control the cost of the initial migration by using the existing hardware efficiently.

Concerning the migration steps, Step 1 necessitates adding tunnel connections, but since there is no change to the backbone network section, and Internet connections are also limited to IPv4 only, we can say that the initial migration is comparatively simple.

In Step 2, we assume full-scale IPv6 deployment with connection to the Internet, but that gives rise to the acquisition of a global IPv6 address, which must be reassigned. Here, based on the record of Step 1, if there is no need to alter administrative policy, the task of alterations entailed by altering router settings is minimized and can proceed smoothly.

As for the number of tasks involved in altering settings, Steps 1 and 2 will each require about one man-month by someone familiar with router settings. In this regard, one method would be to entrust it to the systems integrator who constructed the existing network.

Since many routers can have IPv6 settings added while online, an estimate of suspending the service for about one hour for each firmware upgrade would be sufficient.

(2) Server and client migration

A migration plan must be prepared in order that the migration of servers such DNS, Web and mail will not affect the existing DNS, Web and mail servers already operating in the IPv4 environment. Although a number of tasks required for migration is listed below, we have presupposed the DNS, Web and mail server software, specifically BIND, Apache and Sendmail, to be used for these empirical experiments.

Although there are some differences according to the version of BIND that is currently in use for DNS, the construction of DNS would take a knowledgeable person about one man-day.

Concerning the Web server, although there are some differences according to the current version of Apache, the construction of the Web server would take a knowledgeable person about half a man-day.

The mail server also, although there are some differences according to the current version of Sendmail, the construction of the mail server would take a knowledgeable person about one man-day.

The migration of multimedia application server to IPv6 is broadly divided between the OS section and the application itself.

Concerning the migration of the OS section, if it is an OS such as Windows or Linux, examples of migration to IPv6 appear on Internet sites and a comparatively large amount of information is available in publications, and the general systems integrator can cope with it as normal work.

On the other hand, when it comes to the work of migration and migration of multimedia applications, there will be more cases having application-specific information to be coordinated with information peculiar to the system and OS revision.

If we consider testing the system functions after migration or after system introduction, as well as support during the trial period, the idea of entrusting it to a systems integrator with specialized knowledge including the work of OS migration would be appropriately similar to IPv4.

Apart from that, even if business system applications used within the company migrate to the IPv4/IPv6 dual stack environment, we believe they will still be able to be used as in the existing environment. However, in view of the complete migration to an IPv6 environment as well, we believe a long-term plan must be prepared.

Concerning a PC used in a divisional LAN, if the OS is Windows XP (SP1), typing “ipv6 install” from the command line will make it function as in IPv4/IPv6 dual stack. However, from the idea of peer-to-peer, as an inherent function of Windows XP (SP1), “IPv6 Internet connection firewall” function is sometimes set as a default, and it needs to be turned off at times such as when IP multicast is being used.

If attention is paid to the points given above, we can say that the number of processes required for OS migration is almost negligible.

Concerning the operation of applications, the user will sometimes be aware of whether it is IPv4 or IPv6 that is being used. Nevertheless, we think that when an existing IPv4-compatible application or even an application that has been made compatible with IPv4/IPv6 dual stack migrates, it is preferable that the network environment and applications can migrate seamlessly, with no problems and with the general user not being particularly aware of it.

(3) Internet connection

We can say that to obtain the full benefit from the deployment of IPv6, an Internet connection is essential.

With the model that has now been verified, we are now ready with Step 2 for an IPv6 Internet connection for the first time. Here a valid global address will be obtained, and the IPv6 address for the in-company intranet will be reassigned. These setting changes are not very difficult as they involve only the IPv6 router address that was set in Step 1.

Regular security is generally ensured by a firewall in the Internet settings, but in the verification this time, we have used the router packet filtering function instead of a firewall. If the use of multicast and SIP video telephony is restricted to the intranet, which does not have IPv6 communication with the outside, it is thought to be functionally adequate in this configuration. However, to give full rein to the advantages of IPv6, we must study security modeling for peer-to-peer and routing policy for IP multicast, such as the real need to consider only authorized servers for receiving IP multicast transmissions.

As a connection with specified areas using the Internet, we can also imagine the use of an IPSec tunnel, but in that case this can be done by adding a setting to allow passage with a transmit/receive address.

3.6.2 From the Viewpoint of the Operator

The operator will evaluate and consider whether the safety (assurance of security) and operating efficiency that were achieved by IPv4 have been followed or improved.

(1) Concerning the administration of users

With respect to easy methods of reassigning the IP address of a user’s PC in a large enterprise, whereas under IPv4 it is usually performed by DHCP, in an IPv6 network the general method is to create it automatically from RA and the MAC address of a network interface card. This round of empirical experiments also verified that we were able to reassign addresses simply. In this case, each user and IP address could be related to the MAC address embedded in the interface identifier. However, when an anonymous address is used, which is a characteristic function of IPv6, the terminal periodically changes the address automatically, so we decided that this relationship could not be used.

This matter must be handled as a future problem related to user administration in the IPv6 network and solved quickly.

(2) Concerning the acquisition of a global address

A global address is not necessary in the initial deployment of IPv6, but when the operation was started by defining a temporary address, the work of reassigning at the time of connecting IPv6 to the Internet, from preparation to trial operation, involved tasks of about one hour per network device. Moreover, the network (service) is interrupted during reassignment. This impact and the cost of global address acquisition must be considered in deciding on the timing for acquiring a global address.

If it can be covered with a /48 global address, the present cost of acquisition is about 1000 yen/month, so it would be economical to acquire it at the time of IPv6 deployment

(3) Concerning subnet assignment

Unrelated to the present IPv4 network assignments, we were able to make suitable address allocation for the configuration of the network (system).

At this time, by providing for a case where reassignment has become necessary for some reason, such as starting the operation by defining private addresses on the initial IPv6 deployment and changing to a global address when the IPv6 Internet connection is made, the reassignment could be performed easily by setting up and defining a system for allocating the remaining 16 bits of the network prefix in the /48 global address.

(4) Concerning public servers for IPv6

Regarding the installation of a public server for IPv6, instead of providing a dedicated server, we made the current IPv4 public server into one for IPv4/IPv6 dual stack and had it reference the same content. In this way, instead of managing by committing the same content into an IPv4 public server and an IPv6 public server, we were able to prove that both types could be handled simply with one server.

Moreover, as with the current IPv4 network, we confirmed that security could be ensured by providing transmission to the DMZ and restricting access with a router filter function.

(5) Concerning security

We were able to ensure security by means of access restriction using a router filter function. Actually, in installing an IPv6 public server, the trend of equipment for ensuring security must be widely investigated and the most suitable product at that time must be used.

Moreover, terminals and the like are identified with a global address, and we were able to confirm that when an anonymous address is used, which is a characteristic IPv6 function, so that they do not become targets for attack, the terminal can periodically alter the address automatically. However, as shown in (1) “Concerning the administration of users,” user administration becomes difficult when this function is used. It must be handled as a future problem related to user administration in an IPv6 network and security and solved quickly.

3.6.3 From the Viewpoint of the User

With regard to services that are provided under IPv6, consideration must be given to issues of concern to users, such as when and how the service can be used and the assurance of security concerning the use of global addresses.

(1) Concerning the use of applications

In cases of new applications that can be provided under IPv6, and where applications that are being used under IPv4 have migrated (expanded) to IPv6, we were able to confirm details of services as well as the ranges and development schedules of the services to be provided and that they can be used with confidence.

Depending on the applications in use, we were able to use them at this time without the party with whom we were communicating being aware of IPv4/IPv6, but this awareness was essential in SIP telephony. Therefore, depending on the application, we must pay attention to the need for the other party in the communication to be aware of whether IPv4 or IPv6 is being used.

(2) Concerning security

The use of global addresses is a precondition in an IPv6 network. Therefore, we used global IPv6 addresses in these empirical experiments and we confirmed that we could ensure security by using the router filter function to restrict access. However, to prevent being attacked due to the outflow of terminal address information and successful impersonation, address management by the user also must be considered.

3.7 Issues

Here we shall indicate the issues that have been identified up to now in using the deployment model that was configured in section 3.5.

(1) Anonymous addresses

IPv6 addresses that can be specified on the terminal side include stateless address assignments [8] created automatically from RA and the MAC address of a network interface card, and addresses set manually from the command line interface, and anonymous addresses that the terminal automatically creates and periodically changes.

Concerning these anonymous addresses in particular, it is difficult to identify the terminal from the method of creation of these addresses. Therefore, if they were to be used within the corporation, we expect that the network administrator would have difficulty in controlling the terminals. Moreover, it is conceivable that an operational problem would develop if an application and IPSec were to be used together because of the need for a dynamic change of IPSec policy when the address is changed.

While the existing security policy within the corporation is being taken over, on reconsidering these points, we must also take into account which address should be used in each case.

(2) Security relating to peer-to-peer communications

In the existing IPv4 network environment in a large enterprise, because a function such as NAPT [9] is used to access connections to the outside, basically, connections from the outside cannot be made. Under IPv6, however, because the entire host is in principle a global address, an outsider could try to connect to the host by specifying the direct IPv6 address. One of the forms of communication that uses this is peer-to-peer, but naturally, new security architecture is necessary.

For example, access approval could be established by setting the other party's IPv6 address prefix in the firewall. Also, to make peer-to-peer communication from outside safer would require the migration of a device having a function, such as SIP stateful inspection and firewall devices that provide stateful access approval targeting specified services, are starting to be announced.

(3) Fallback to IPv4

It should be noted that under an IPv4/IPv6 dual stack environment, the standard arrangement at present for operating an application that is only IPv6-compatible is to pass on the IPv6 address of the DNS server. At present, there are the following two responses:

- Access the DNS with IPv4, using the IPv4 function of the OS.
- Do not use the DNS server.

Also, under an IPv4/IPv6 dual stack environment, a method [10] of accessing the DNS server with an IPv4/IPv6-dual-compatible application is also being proposed. If an IPv4/IPv6-dual-compatible application is announced separately, this point should be considered.

This item will be reviewed through the establishment of the DNS server's IPv6 address notification method.

(4) IP multicast

Although loading multicast with IPv6 is proceeding, there is a number of points that need to be considered.

One is related to traffic characteristics. With IPv6 multicast, in many cases it can be used for the distribution of streaming traffic, but because it uses UDP, retransmission and convergence are unavailable. Moreover, because it uses the bandwidth continuously, a performance unlike the previous one is required. In other words, in selecting a router for IP multicast, handling capacity must be thoroughly considered. Furthermore, among streaming servers, there are some that momentarily generate high bursting traffic that greatly exceeds the encode rate, and in that case can impart a major load on the network. In IPv6 multicast applications, there are some that generate traffic at several tens of Mbps and, based on these facts, it is possible that in an ordinary corporation usage, up to several Mbps would be appropriate.

Next is the consideration of security. With regard to the security of IP multicast, there are some parts that are not sufficiently implemented and firewalls that are compatible with PIM-SM and MLD, which are standard routing protocols, have not yet been released. Concerning that system, there are access controls on routing protocols for multicast groups and server source addresses as well as filter functions for blocking the actual multicast data.

Furthermore, concerning whether or not the content itself can be viewed, there is digital rights management (DRM), but there seem to be few if any examples of DRM having been implemented with IP multicast transmission. If one is considering the use of IP multicast, the migration of this technology should also be considered.

With the verification this time, broadband transmission is enabled by using a router with an IP multicast transmission experiment record [11] and a streaming server with comparatively little bursting. As a switch-compatible function, IGMP snooping [12] is often implemented as an IP multicast data streaming control for IPv4, and equipment has started to be released that has functions compatible with IPv6 MLD. The use of these is less expensive, and IP multicast-compatible networks can probably be constructed.

References

[1] http://www.isc.org/

[2] http://www.sendmail.org/jp/

[3] http://www.apache.jp/

[4] A. Conta et al. "Generic Packet Tunneling in IPv6 Specification," RFC 2473, 1998

[5] A. Durand. "Operational Considerations and Issues with IPv6 DNS," draft-ietf-dnsop-ipv6-dns-issues-04.txt

[6] J. Rosenberg et al. "SIP: Session Initiation Protocol," RFC 3261, 2002

[7] D. Estrin et al. "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification," RFC 2362, 1998

[8] S. Thomson et al. "IPv6 Stateless Address Autoconfiguration," RFC 2462, 1998

[9] P. Srisuresh et al. "IP Network Address Translator (NAT) Terminology and Considerations," RFC2663, 1999

[10] Myung-Ki Shin. ”Application Aspects of IPv6 Transition," draft-ietf-v6ops-application-transition-01.txt, 2004

4. Guideline for Small and Medium-Sized Enterprise Segment

4.1 Overview

4.1.1 Aim of this Guideline

This chapter of Part 2 presents a guideline for IPv6 deployment for small and medium-sized enterprises. In this chapter, we built a model case environment for the initial stage of IPv6 deployment. In introducing specific deployment methods for the changeover to IPv6 in that environment, we describe solutions we actually implemented, merits we realized, and outstanding issues. While the main target of this chapter is small and medium-sized enterprises, the scope of use extends to general-use sectors and takes into account nationwide offices of large enterprises which possess network systems similar to those found in small and medium-sized enterprises, small sales offices and convenience stores, as well as head office networks and network system providers (ISPs, ASPs, etc.) to which these network systems are connected.

This chapter also presents details confirmed on the basis of verification results of analyses and issues in the Deployment Guidelines for the Small Office/Home Office (SOHO) Segment by the Deployment Working Group of the IPv6 Promotion Council (hereinafter referred to as “Deployment WG Guidelines”).

4.1.2 Typical Deployment Scenario for Small and Medium-Sized Enterprise Networks

We used the Deployment WG Guidelines as our reference for a typical deployment scenario for a small and medium-sized enterprise (SOHO) network. According to the guidelines, the deployment period is divided into three phases:

- IPv4 current usage period
- Initial IPv6 introduction period
  - IPv6 for a specific purpose
  - IPv6 full-scale introduction
- Full-scale IPv6 propagation period

The deployment described in this chapter focuses on how IPv6 will be introduced into existing IPv4 systems. Therefore, both a specific purpose model and a full-scale introduction model were formulated and examined for the initial IPv6 deployment phase.

4.1.3 IPv6 Deployment Scenarios

Specific Purpose Model

The specific purpose model is one that introduces a system utilizing IPv6 for specific business purposes where, for example, multicast or end-to-end communications are desired. A typical example is a model that selects IPv6 as an easy means for realizing the construction of the environment required for peer-to-peer communication with IP phones. In terms of IPv6 deployment, this is a very limited form of introduction.

Among the characteristics of this system are:

- The establishment of IPv6 usage is limited to specific applications.
- IPv6 and IPv4 coexist at the terminal level.
- Care is taken to avoid any impact on the existing system (with IPv4 still in operation).

The following are examples of areas where IPv6 may be applied:

- Applications where there are restrictions on functions or communications due to NAT

  Examples: IP phones, instant messaging
- Applications that require security between terminals

  Examples: extranet, remote service maintenance

Full-scale Deployment Model

The full-scale model is one where IPv6 propagation is anticipated in the future and where IPv6 can be made available for each system at the time the existing system is being replaced. In this model, although there are no IPv6 benefits at present for Web browsing or mail, the system is built to support IPv6. In comparison with the model for a specific purpose, it can be said that this is a more forward-looking model for the deployment of IPv6.

However, in terms of IPv6 packaging in current products and applications, there are still areas in systems that cannot support IPv6. Therefore, at this stage, an environment where both IPv4 and IPv6 can coexist is required for both models.

4.1.4 Flow for the Deployment of IPv6

Figure 4.1.4.1 shows the flow for IPv6 deployment in future deployment models where almost all communication is conducted over IPv6.

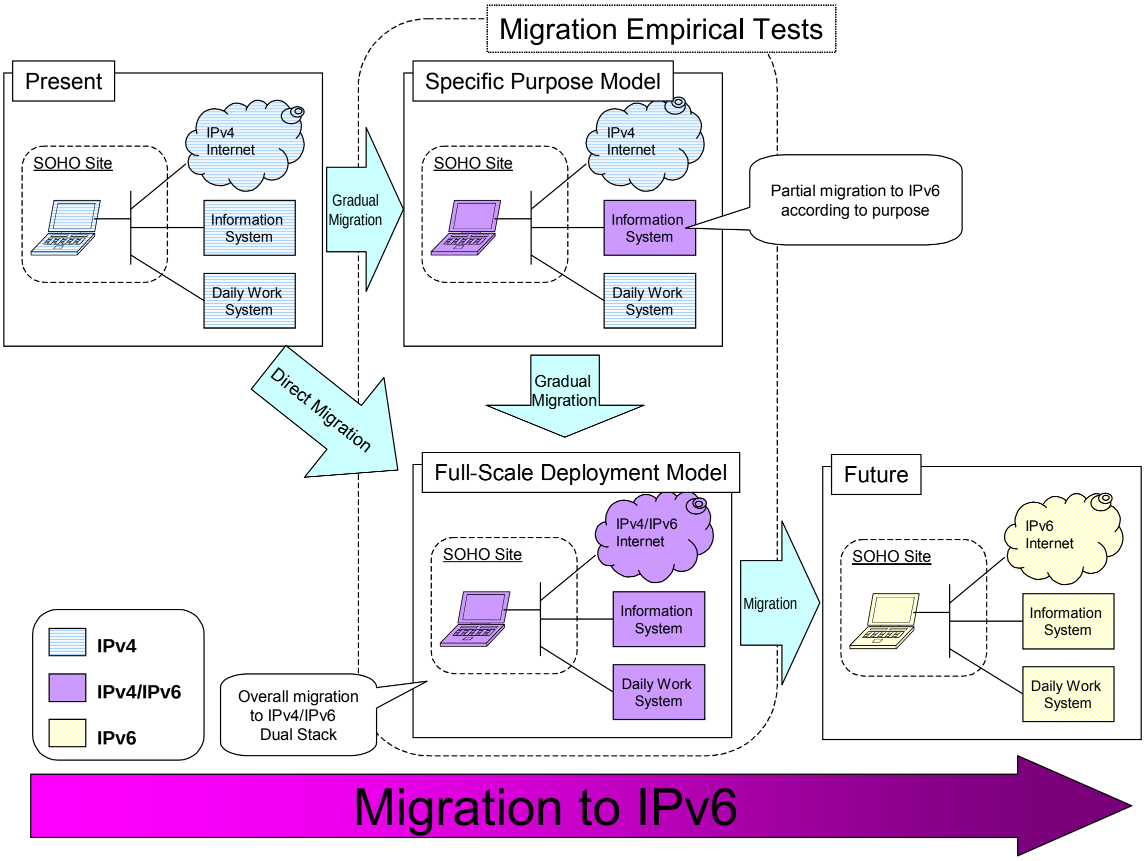


Figure 4.1.4.1: Gradual Migration to IPv6

4.2 Small Office/Home Office (SOHO) Network Model

The Deployment WG Guidelines categorize SOHO networks into four different types:

- Family operations
  - Consisting of one PC and Internet connection line
- Small business offices (independent SOHO)
  - Consisting of several PCs and a single LAN sub network, in addition to configurations at family operations
  - Examples: law offices, architecture offices
- Small sales offices (dependent SOHO)
  - Small business offices belonging to a company group; in many cases, VPN or other means is used to connect to the main office or ASP center.
  - Examples: travel agents, insurance offices
- Convenience stores
  - Equipment includes POS terminals and non-PC terminals; the network configuration often has an original environment.

In Part 2, as our model, we decided to examine dependent SOHOs, a model targeted for deployment investigation in the Deployment WG Guidelines, from two perspectives:

- as a model encountered frequently in networks
- as a model that could be examined with independent SOHOs

4.2.1 Dependent SOHO Network

The following is a typical example of a dependent SOHO network.

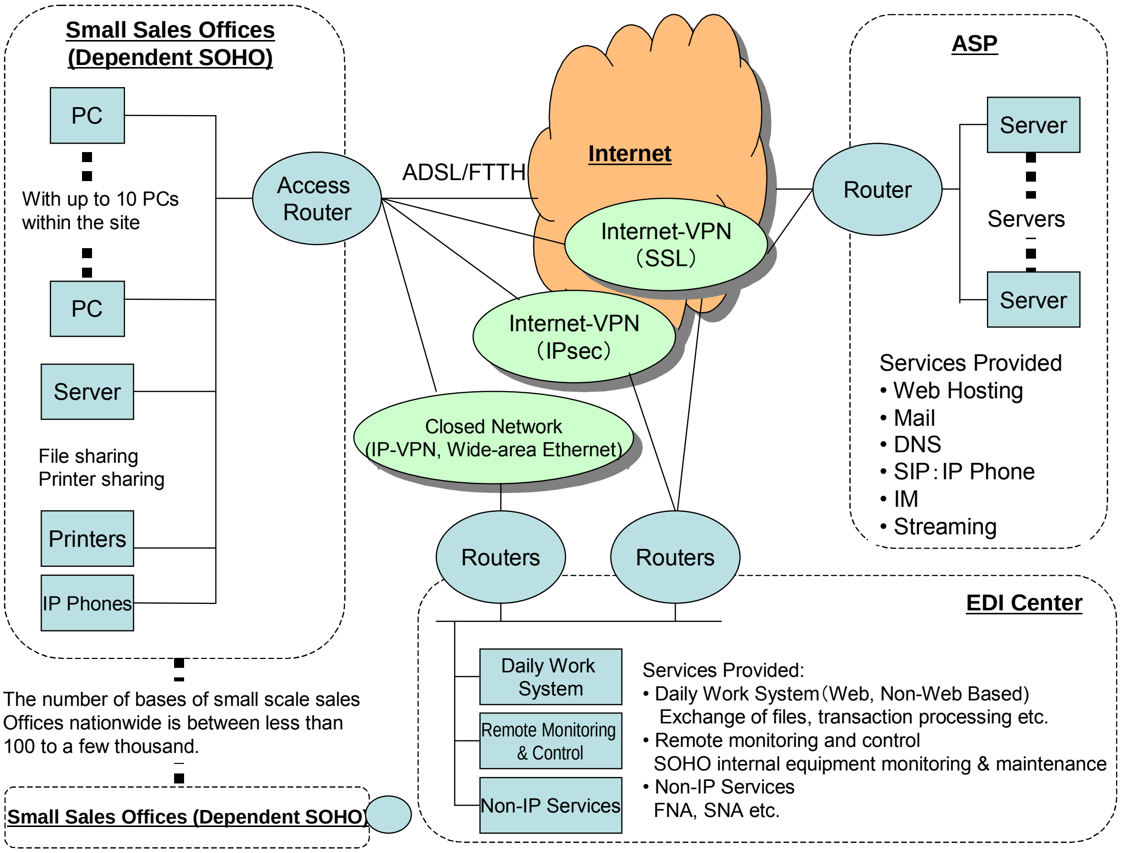

Small Sales Offices (Dependent SOHO)
PC
With up to 10 PCs within the site
PC
Server
File sharing
Printer sharing
Printers
IP Phones
Access Router
ADSL/FTTH
Internet
Internet-VPN (SSL)
Internet-VPN (IPsec)
Closed Network (IP-VPN, Wide-area Ethernet)
Routers
Routers
ASP
Router
Server
Servers
Server
Services Provided
• Web Hosting
• Mail
• DNS
• SIP : IP Phone
• IM
• Streaming
EDI Center
Daily Work System
Remote Monitoring & Control
Non-IP Services
Services Provided:
• Daily Work System (Web, Non-Web Based)
Exchange of files, transaction processing etc.
• Remote monitoring and control
SOHO internal equipment monitoring & maintenance
• Non-IP Services
FNA, SNA etc.
The number of bases of small scale sales Offices nationwide is between less than 100 to a few thousand.
Small Sales Offices (Dependent SOHO)

Figure 4.2.1.1: Typical Example of a Dependent SOHO Network

This network, divided according to functions, consists of the following three subsystems:

- Dependent SOHO site
- ASP (Application Service Provider)
- EDI (Electronic Data Interchange) center

The following section gives a detailed description of each subsystem.

The Dependent SOHO Site

The SOHO site, by nature, is small in scale and has a large number of bases. Therefore, it selects lines that are inexpensive and easy to install. Recently, broadband access lines, such as ADSL, and Internet use are becoming commonly used. As a result, relatively inexpensive access routers are used in the communications equipment.

PCs are predominantly used as terminals for sites such as this. A large number, approximately 10 or so, are used. In some cases, the server is set up for file sharing and printer sharing. Other terminals may include business equipment such as printers.

Recently, new types of equipment, such as IP phones, are also beginning to appear.

ASP

The ASP is the center for providing services to the SOHO site user. The types of services provided are mainly information services and include mail and Web hosting. Recently, SIP servers with IP phones are included in these services.

EDI Center

This is the center that provides mainly business applications for the SOHO. The services it provides include file exchange and transactions. There are also services that cannot be accessed by IP, but recently, Web-based systems are becoming the main means for providing these services.

Furthermore, the terminals used at sites like this in many cases are distributed by the main office servicer that provides the business service. Therefore, the maintenance and monitoring services of the terminals are also sometimes provided by the same servicer.

4.2.2 Applications Used

Descriptions of the applications used in the dependent SOHO are roughly classified and described below.

Information Applications

These are the applications that are provided by the ASP mentioned above. They consist mainly of mail and Web browsing applications. Other applications include IP phones, videoconferencing, instant messaging, and video streaming.

Business Applications

These are the business applications required to conduct SOHO business on a daily basis and include, for example, receiving and placing orders from sales outlets, inventory confirmation, and reporting sales to the main office.

Management-related Applications

These are applications for managing the SOHO site and include, for example, monitoring, terminal management, and updating software.

4.2.3 Ensuring Security

As previously mentioned, there are many ways in which services are accessed via the Internet. To safeguard security at such times, it is essential to:

- keep communications concealed
- eliminate unauthorized access

As ways of concealing communications, the following are typical methods currently used:

- the establishment of a VPN using IPsec
- the use of an SSL connection to the Web server

While IPsec can support multiprotocols, when an SSL is used, the area that can be accessed is restricted, for example, to Web access.

As a means of avoiding unauthorized access, firewall tools at the terminal level are now available, but the security functions of access routers are generally used at present. The SOHO network is protected by setting access restrictions to the internal network in the router using packet filters and NAT. Recent access routers also sometimes have simple IDS functions, so their use can also be considered.

4.3 Practical Example of IPv6 Deployment

The following section gives an account of a configuration we built as a model dependent SOHO network.

4.3.1 Prior to IPv6 Deployment

Figure 4.3.1.1 shows the configuration of the model. The server and network equipment that support IPv6 do not exist. In this model, two types of communication were assumed. One was communication to the information center's Web server or mail server from a SOHO site user terminal; the other was communications to various EDI Center servers from a SOHO site business terminal. A connected Internet network was used for Internet communication from each site. In addition, the use of an Internet VPN was assumed for establishing security where it was required.

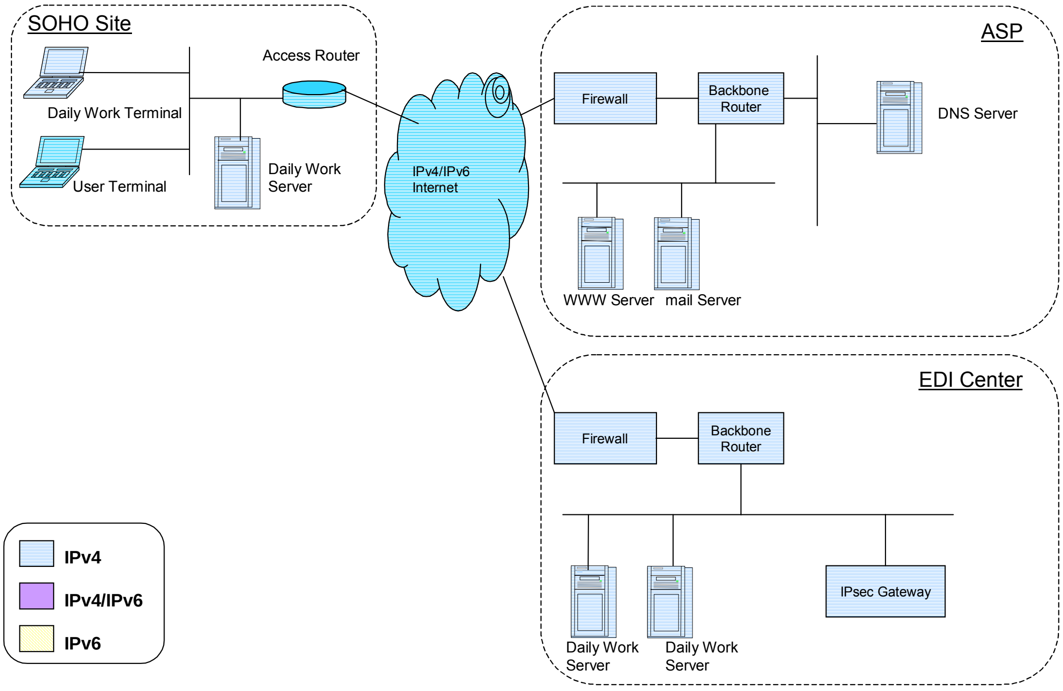


Figure 4.3.1.1: Example of a Typical Existing Configuration

4.3.2 IPv6 Deployment Period 1 (Specific Purpose Model)

An example of the configuration of this model is shown in Figure 4.3.2.1. In this deployment model, IPv6 is introduced for use in communications where IPv6 is particularly effective (real-time communications, etc.). The only equipment on the communication path that supports IPv6 is the equipment that is required for IPv6-based communications. Work communications that do not particularly require changing to IPv6 use the existing IPv4 protocol.

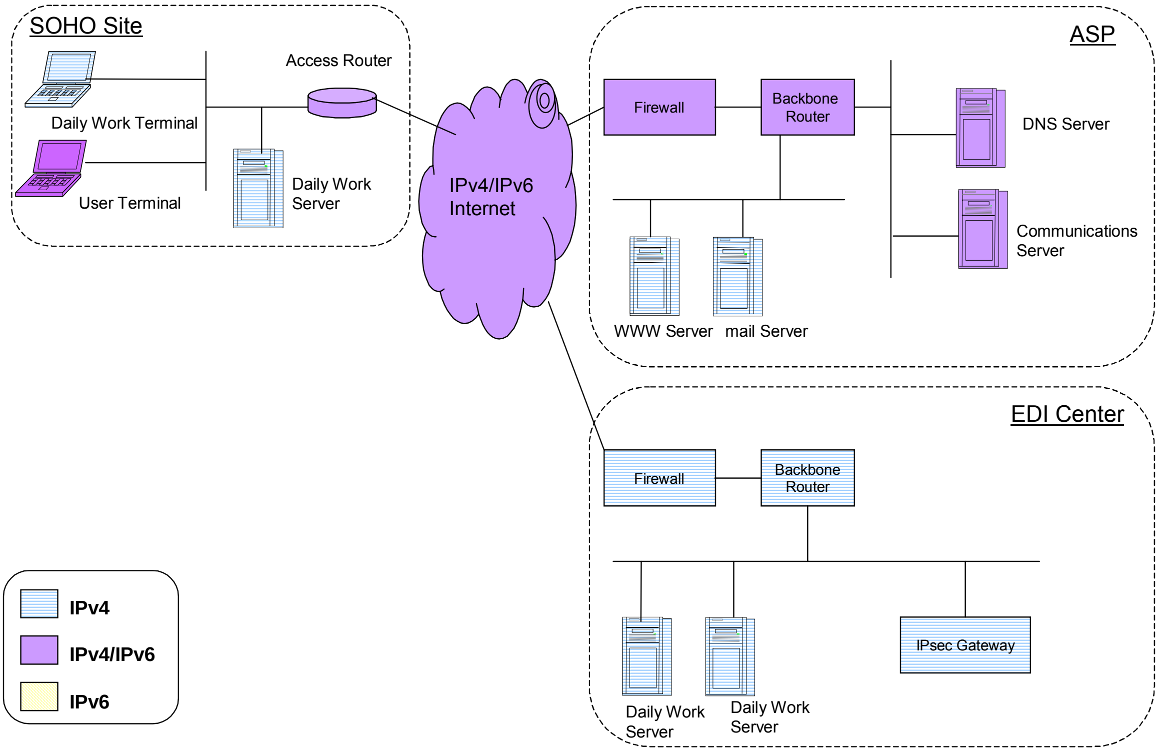


Figure 4.3.2.1: Specific Purpose Model

4.3.3 IPv6 Deployment Period 2 (Full-scale Model)

An example of the configuration of this model is shown in Figure 4.3.3.1. This deployment model is introduced for the use of IPv6 as the standard environment. Almost all communications migrate to IPv6, but there are some remaining IPv4 communications, such as IPv4 Internet Web sites. In addition, a proxy and translator are used for mutual communication between IPv4 and IPv6.

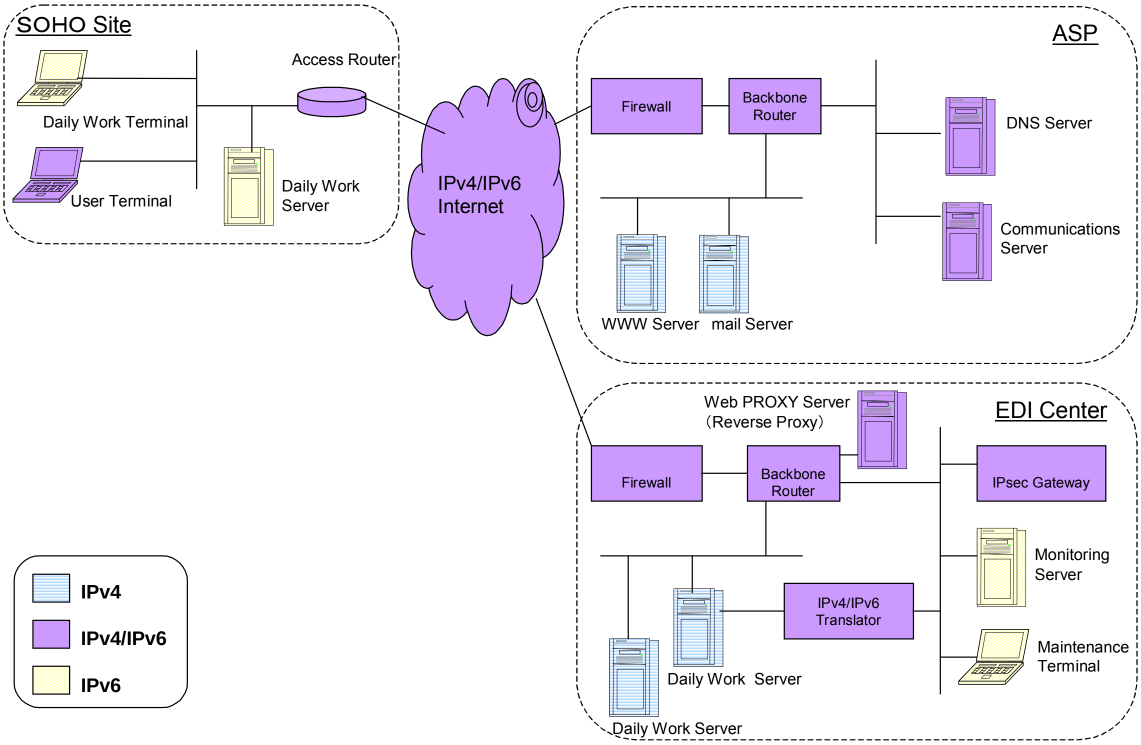


Figure 4.3.3.1: Full-scale Deployment Model

4.4 Verification and Evaluation of Model Cases

The actual environments were built in the above assumed model cases, and their operation was confirmed.

The equipment configuration is shown in Table 4.3.3.1.

Table 4.3.3.1: Equipment Configuration

No.	Installation Site	Name of Device	Specifications	OS/Software	IPv4 Address	IPv6 Address	Notes
1	Site A	Access Router	GeoStream Si-R170	-	10.3.1.2	2001:db8:3000:115::1:1	LAN Address
					192.0.2.130	2001:db8:3000:111::1:2	WAN Address
2		Access Router	GeoStream Si-R170	-	10.3.1.3	2001:db8:3000:116::1:1	LAN Address
					192.0.2.131	2001:db8:3000:112::1:2	WAN Address
3		Business Server	PRIMERGY RX100	Windows Server 2003	10.3.1.101	2001:db8:3000:115::1:101	
4		User Terminal	FMV-BIBLO MG70E	Windows XP Professional	DHCP auto allocation	RA auto allocation	
5		Business Terminal	FMV-BIBLO NB50E	Windows XP Home Edition	DHCP auto allocation	RA auto allocation	
6		Wireless Mobile Terminal	Pocket LOOX	Windows Mobile 2003	DHCP auto allocation	RA auto allocation	
7	Site B	Access Router	GeoStream Si-R170	-	10.3.3.1	2001:db8:3000:135::1:1	LAN Address
					192.0.2.134	2001:db8:3000:131::1:2	WAN Address
8		User Terminal	FMV-BIBLO MG70E	Windows XP Professional	DHCP auto allocation	RA auto allocation	
9	ASP	Firewall	PRIMEPOWER1	Solaris Operating Environment, Interstage Security Director V5.1	192.0.2.162	2001:db8:3000:211::1:2	Internet Address
					192.0.2.177	2001:db8:3000:212::1:1	DNS Server Address
					192.0.2.185		WWW Server Address
10		Backbone Router	GeoStream R920	-	192.0.2.153	2001:db8:3000:1::1:2	Firewall Address for ISP Segment Connection
					192.0.2.145	2001:db8:3000:2::1:1	Internet Address
					192.0.2.129	2001:db8:3000:111::1:1 2001:db8:3000:112：:1:1 2001:db8:3000:121：:1:1 2001:db8:3000:122：:1:1 2001:db8:3000:112：:1:1 2001:db8:3000:131：:1:1 2001:db8:3000:141：:1:1	Internet Address
11		WWW Server		RedHat Linux 9 Apache HTTP server 2.0.48 Tomcat-4.1.29 J2SDK 1.4.2_03	192.0.2.178		
12		mail Server		RedHat Linux 9 Sendmail 8.12.10 Qpopper 4.0.5 Uw-imap 2002d	192.0.2.179		

13		DNS Server	PRIMERGY RX100	RedHat Linux 9 Bind-9.2.3	192.0.2.186	2001:db8:3000:212::1:2	
14		SIP Server	PRIMEPOWER250	Solaris Operating Environment, GeoServe/SIP	192.0.2.187	2001:db8:3000:212::5060	
15		IM Server	PRIMEPOWER250	Solaris Operating Environment, GeoServe/IM	192.0.2.188	2001:db8:3000:212::5061	
16	EDI Center	Firewall	PRIMEPOWER1	Solaris Operating Environment, Interstage Security Director V5.1	192.0.2.146	2001:db8:3000:2::1:2	Internet Address
					192.0.2.193	2001:db8:3000:311::1:1	Backbone Router Address
17		Backbone Router	GeoStream R920	-	192.0.2.194	2001:db8:3000:311::1:2	Firewall Adress
					192.0.2.197	2001:db8:3000:312::1:1	Web Proxy Server Address
					192.0.2.209	2001:db8:3000:313::1:1	Monitoring Server Address
					192.0.2.217	2001:db8:3000:315::1:1	Business Server Address
18		Web Proxy Server	PRIMERGY RX100	RedHat Linux 9 Apache HTTP server 2.0.48	192.0.2.198	2001:db8:3000:312::1:101	
19		IPv4/IPv6 Translator	IPCOM300	-	192.0.2.202	2001:db8:3000:314::1:2	IPsecGW Address
					192.0.2.220	2001:db8:3000:315::1:2	Business Server Address
20		Monitoring Server	PRIMERGY RX100	RedHat Linux 9	192.0.2.210	2001:db8:3000:313::1:101	
21		Maintenance Terminal	LOOX T70	Windows XP Home Edition	192.0.2.211	RA auto allocation	
22		IPsec Gateway	Si-R500	-	192.0.2.212	2001:db8:3000:313::1:2	Backbone Router Address
					192.0.2.201	2001:db8:3000:314::1:1	IPv4/IPv6 Translator Address
23		Business Server (Web-based)	PRIMERGY RX100	RedHat Linux 9 Apache HTTP server 2.0.48	192.0.2.218	2001:db8:3000:315::1:101	
						2001:db8:3000:325::1:101	v4/v6 Conversion Address
24		Business Server (Non-Web)	PRIMERGY RX100	Windows Server 2003 Exchange Server 2003 Openssh	192.0.2.219	2001:db8:3000:315::1:102	
						2001:db8:3000:325::1:102	v4/v6 Conversion Address
25	Wireless	Wireless Mobile Terminal	Pocket LOOX	Windows Mobile 2003	DHCP auto allocation	RA auto allocation	

4.4.1 Network Configuration

This section describes the evaluation of the network configuration and points that should be taken into consideration.

IP Address Configuration

In this trial, the configuration of the Deployment Working Group was used as a reference for the IP address settings, and they were set according to the following configuration:

- LAN addresses with a dual stack configuration
- LAN IPv6 address prefix length

- Automatic settings for addresses to terminals

The automatic settings for communications and addresses were confirmed using this configuration.

Since there was dual stacking, for the automatic settings for addresses, DHCP was used for IPv4 and RA for IPv6. There were no problems at the time of verification, and by following the manual, we were able to make the settings for the terminals and the routers. In a simple environment like SOHO, as in IPv4, there are no major problems in producing IP address-related configurations.

However, we used Windows XP and we were not able to confirm whether the IPv6 addresses were obtained normally in the standard dialog box. This could be because IPv6 is based on Plug and Play where there is a policy of refraining from revealing settings to the user wherever possible. To confirm that addresses are obtained, it is possible to open the DOS-Prompt and confirm the address acquisition status, but it is probably preferable for the systems integrator or operator to have an operation tool to make confirmation more convenient at the time of construction and operation.

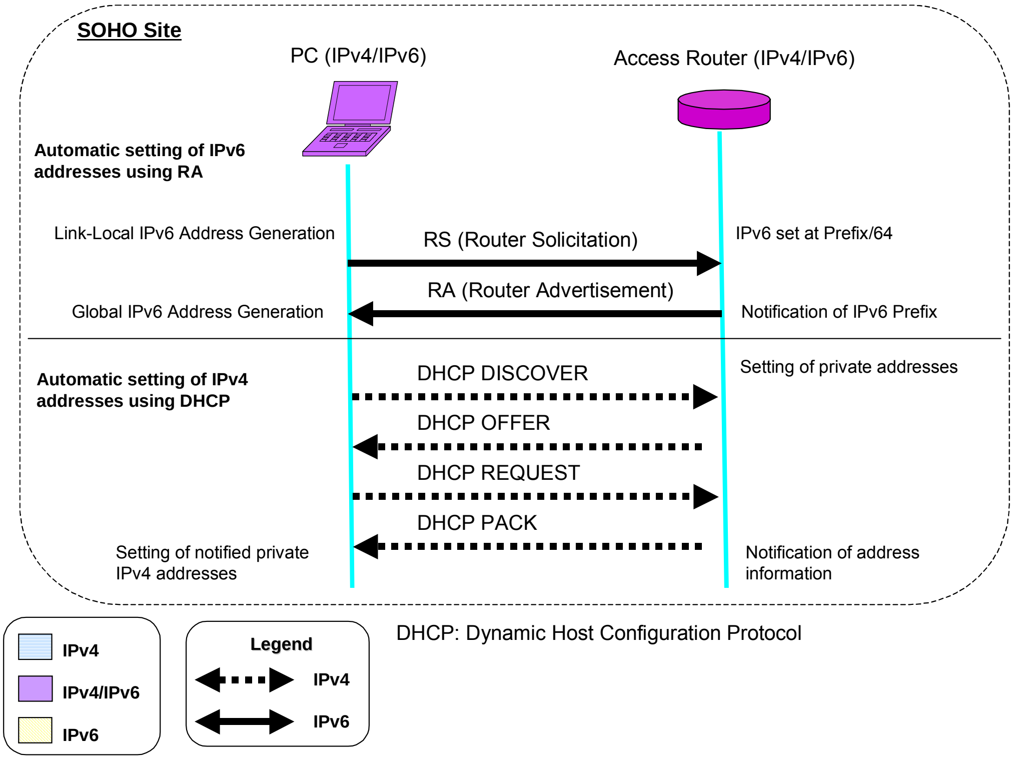

SOHO Site
PC (IPv4/IPv6)
Access Router (IPv4/IPv6)
Automatic setting of IPv6 addresses using RA
Link-Local IPv6 Address Generation
RS (Router Solicitation)
IPv6 set at Prefix/64
RA (Router Advertisement)
Global IPv6 Address Generation
Notification of IPv6 Prefix
Automatic setting of IPv4 addresses using DHCP
DHCP DISCOVER
Setting of private addresses
DHCP OFFER
DHCP REQUEST
DHCP PACK
Setting of notified private IPv4 addresses
Notification of address information
IPv4
IPv4/IPv6
IPv6
Legend
IPv4
IPv6
DHCP: Dynamic Host Configuration Protocol

Figure 4.4.1.1: Overview of IP Address Configuration

Forming Links

In the Deployment WG Guidelines, two methods are given for the formation of links to the SOHO site:

- Native connection method
  This method establishes IPv6 communications using an IPv4/IPv6 dual stack line provided by the ISP or Network Administrator.
- Tunnel connection method
  This method establishes a tunnel from the IPv4 access router for the gateway that is installed by the ISP or Network Administrator, and IPv6 communications are established on top of that.

For the verification, we adopted a native connection to form a link to the SOHO site and configured the network.

Currently, the automatic prefix delegation function for IPv6 addresses to sites is generally supported by ISPs that provide native connection services. However, because of the trials we were conducting, on this occasion we did the network configuration without using this function.

To confirm the effects of using a dual stack line, we verified both IPv4 and IPv6 communications and compared their efficiency in throughput, delay and other areas. Results showed that there was no particularly definitive difference in efficiency between the two.

This means that if, for example, lines in an existing IPv4 LAN system are made to support IPv6 through dual stacking, the existing system can continue to be used unaffected. In this way, an IPv6 system can probably be introduced as a supplement to the existing system.

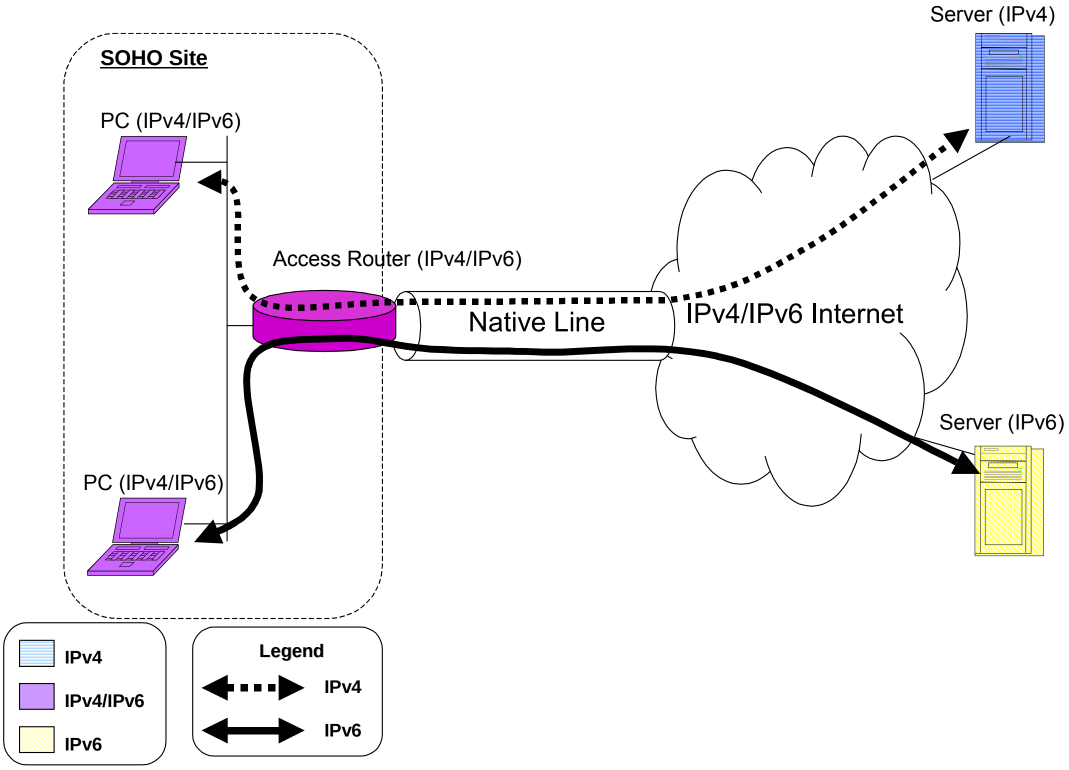


Figure 4.4.1.2: Overview of a Link Configuration Using a Native Connection

Equipment Configuration

The following equipment was used to confirm the configuration:

- Router: Fujitsu GeoStream Si-R170
- Terminal: Fujitsu FMV-BIBLO MG70E (Windows XP Professional)

This is exactly the same configuration that is generally used in SOHO IPv4 environments. To achieve this configuration, no operations such as updating the OS were required. Although requirements will vary with the environment and the equipment, this essentially means that the latest equipment currently available is used, and no additional capital investment is required to construct an IPv6 system. Since little equipment is used in the SOHO and the scope of the environment can be specified, the IPv6 environment is relatively easy to achieve.

To build the IPv6 communications environment, we made the settings for the terminals and the routers. We conducted the operations according to the manual and were able to make the settings through ordinary network construction and following the same flow. In the course of making the settings, however, we encountered various terms specific to IPv6, such as “router advertisement” and “RIPng”. In addition, special

IPv6-specific address settings to the router were required. Therefore, a certain level of preliminary knowledge regarding IPv6 is required beforehand for making the settings.

Summary of the Network Configuration

In summary, the points that have been made thus far concerning the network configuration are:

- The deployment of IPv6 has no impact on the use of IPv4 communications.
- IPv6 construction requires no special equipment.
- Special, complex operations are not involved in making IPv6 settings.
- A basic, preliminary knowledge is required in IPv6 construction

While circumstances vary according to the environment and while sweeping generalizations cannot be made, it can be said that on the whole there are no major problems in the deployment of IPv6.

4.4.2 Migration of Applications

This section describes the evaluation of the network construction and points that should be taken into consideration.

Target Applications

As we explained earlier in the section on models, we confirmed the use of the following applications in an IPv4/IPv6 dual stack environment:

- Web browsing (of Internet content)
- Mail
- Peer-to-peer applications
- IP phones / Instant messaging
- Web-based work applications
- Proprietary applications
- Monitoring systems

Web Browsing

The Deployment Working Group has been recommending that in the current environment, the existing IPv4 is fine as is for browsing. Keeping this point in mind as a reference, in this verification we were able to confirm that IPv4 browsing presented no problems in a dual stack environment. To compare the environment with an IPv4 single stack environment, we compared the same content and did not perceive any real differences between the two.

At present, in terms of Internet use, almost all Web sites are in fact IPv4, so there will be many cases in which the same environment that we used for this verification will occur. Since we were not able to perceive any differences in use during browsing, the end user will probably not be aware of the dual stacking of the network. In terms of Web browsing, we believe that the deployment of IPv6 will not have any impact on actual business or on usage.

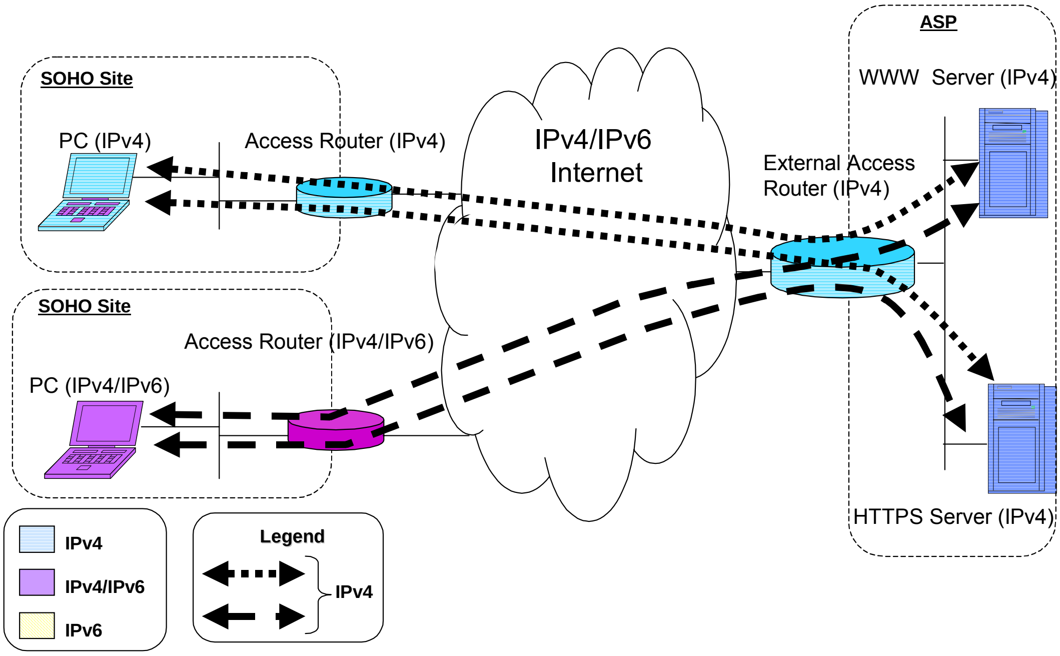


Figure 4.4.2.1: Web Browsing Overview

Mail

We also confirmed mail communications using IPv4 in a dual stack environment. Using mail that utilizes the most generally used SMTP/POP, we confirmed the sending and receiving of text mail and mail with attachments, but found no particular differences from an IPv4 environment. Like Web browsing, there will probably be no impact on mail use from the user’s point of view.

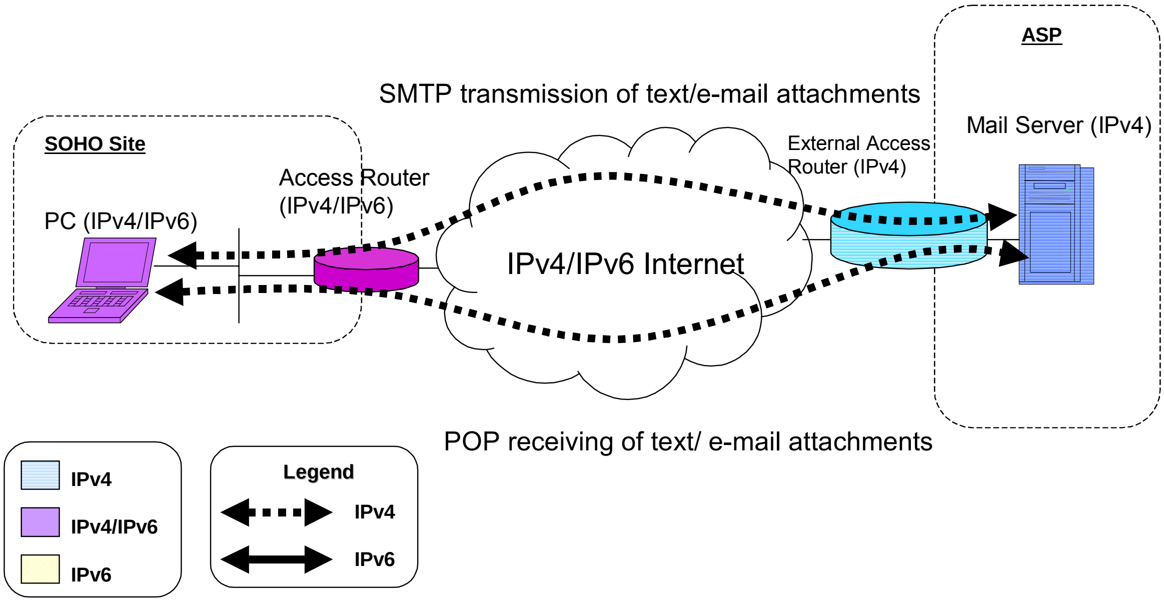

ASP
SMTP transmission of text/e-mail attachments
Mail Server (IPv4)
SOHO Site
External Access Router (IPv4)
Access Router (IPv4/IPv6)
PC (IPv4/IPv6)
IPv4/IPv6 Internet
POP receiving of text/ e-mail attachments
IPv4
IPv4/IPv6
IPv6
Legend
IPv4
IPv6

Figure 4.4.2.2: Overview of Sending and Receiving Mail

The results of our evaluation of Web browsing and mail indicate that the deployment of IPv6 poses no particular problems for general Internet use.

Web-based Business Applications

On this occasion, we evaluated the Web access functions of Microsoft Exchange using Web applications for use in SOHO business.

The Deployment Working Group mentions the possibility that IPv6 may be used for business applications. Therefore, we decided to conduct evaluations of this configuration in both IPv6 and IPv4.

To determine whether IPv6 would be supported, we conducted verifications of the following two patterns as Web service server configurations supporting IPv6:

(A) Use of a server supporting IPv6

(B) Use of the existing IPv4 server and IPv6 ALG (reverse proxy)

We checked the schedule at the exchange, including the use of IPv4, and verified and compared the transmission and receipt of mail and whether or not the above patterns could be used. Our results confirmed that both were possible.

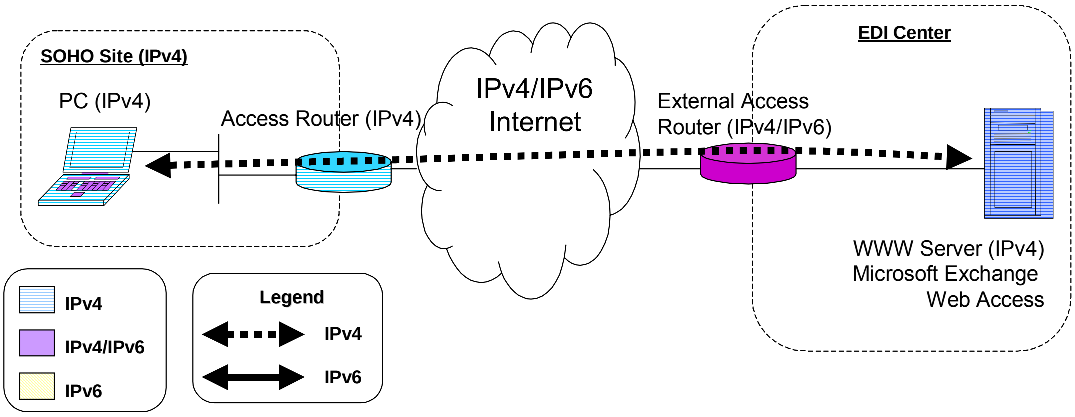


Figure 4.4.2.3: Overview of Use with Web-based Business Applications (IPv4 Server)

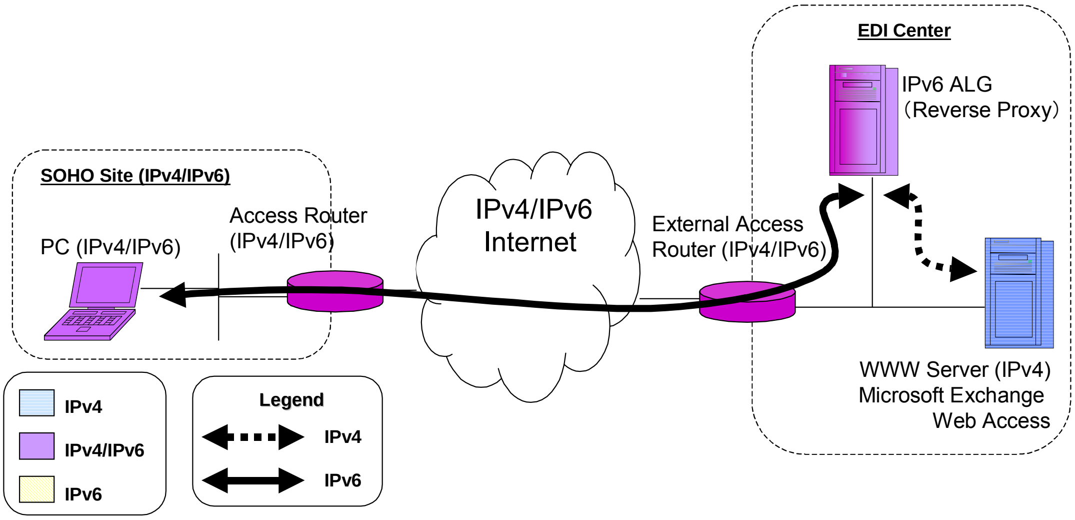


Figure 4.4.2.4: Overview of Use with Web-based Business Applications (IPv6 ALG)

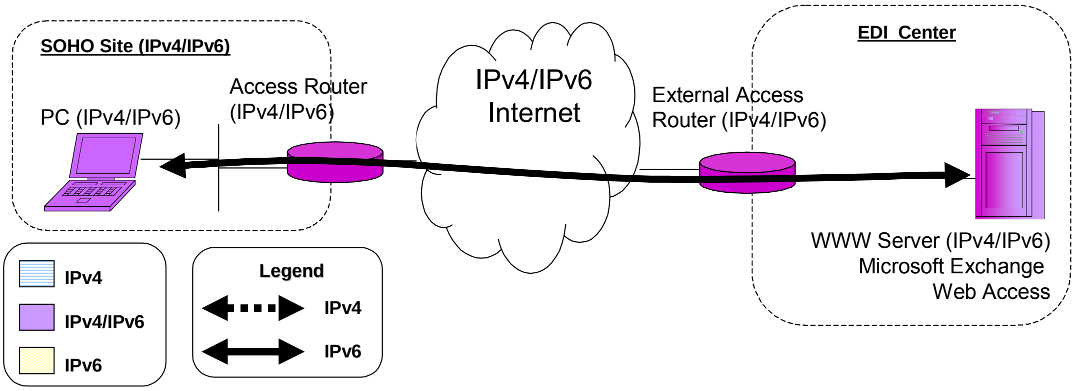


Figure 4.4.2.5: Overview of Use with Web-based Applications (IPv4/IPv6 Server)

Both IPv6 ALG and a server supporting IPv6 can be recommended as configurations that can be used. Of the two, however, the ALG pattern is recommended as an operable form that will not have much impact on existing services.

When ALG is used, however, it has certain requirements that may be seen as disadvantages that inhibit its introduction:

- An additional server is required, resulting in increased costs
- Server settings are required, resulting in increased operations

Actually, when ALG is used, a number of slightly complicated settings is required for responding with reverse proxy IPv6 addresses at the time of the name resolution of the Web server's true host name at the DNS server. In any event, introduction must be considered on a case-by-case basis, taking into account various factors, such as the original configuration and costs.

Verification was not performed for this configuration, though server load sharing devices supporting IPv6, such as f5 Network's "Big IP," are beginning to become available. There are probably already cases in which centers have actually been built using products like this, so IPv6 support through load-sharing devices will probably come to the fore as a possible candidate for configuration.

Proprietary Business Applications

Here we used FTP and Microsoft Exchange Server to verify non-Web IP applications used in SOHO business.

In IPv4, communications are protected through the use of IPsec communications using routers and other means. However, in this case, we built an IPsec communications environment from the terminal with a view to utilizing an IPv6 end-to-end communications environment and conducted verifications.

The results indicated a number of problems. The following two points summarize the problems:

(1) IPsec implementation

For the initial test environment, we planned to execute IPv6 IPsec communications using Windows XP IPsec Client for the terminal and IPsec GW made by Fujitsu for the server. However, the following problems occurred:

- IPsec connection between the IPsec client and the GW was not possible.
- IKE and encryption at the IPsec client were not executed.

Therefore, we changed the server to one using FreeBSD instead of GW and conducted verifications without making settings for IKE and encryption. As a result, we were able to confirm communications.

While we were not able to verify the encryption at this time, IPsec encrypted communication was possible using the product "MyNetManager." It is our belief that the problem was at the product level. IPsec problems in compatibility also occur with IPv4, so it cannot be considered a problem experienced solely with IPv6. It is an area where technical improvements are expected in the future.

(2) Non-support of IPv6 at the Application Level

We attempted to verify synchronization of the Microsoft Exchange and Outlook schedules, but we were not able to establish a connection. The communications protocol (rpc) used in Microsoft Exchange is IPv6 at the OS level. However, IPv6 is not supported at the applications level and consequently, our verifications did not proceed smoothly. FTP was among the communications that we did confirm, and we encountered no problems in that area.

In summarizing details in this area, we believe that attention must be given to the following points:

- Even when there are claims of IPsec and other function support, the level of support varies.
- Mutual connections for complex functions cannot be determined without function verification.
- There are differences in the level of IPv6 support in proprietary applications.

The above problems are also problems that can occur in IPv4. However, IPv6 is a technology that is currently being propagated and, consequently, there is a possibility that such problems will occur with greater frequency.

Furthermore, in proprietary applications, there are many areas where specific details regarding support are difficult to identify. This area requires particular attention.

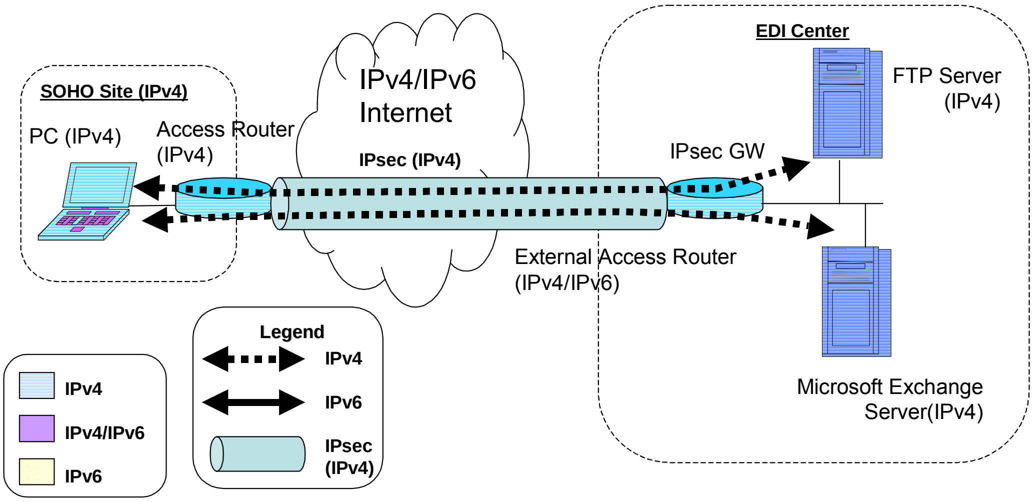


Figure 4.4.2.6: Overview of the Use of Proprietary Business Applications (IPv4)

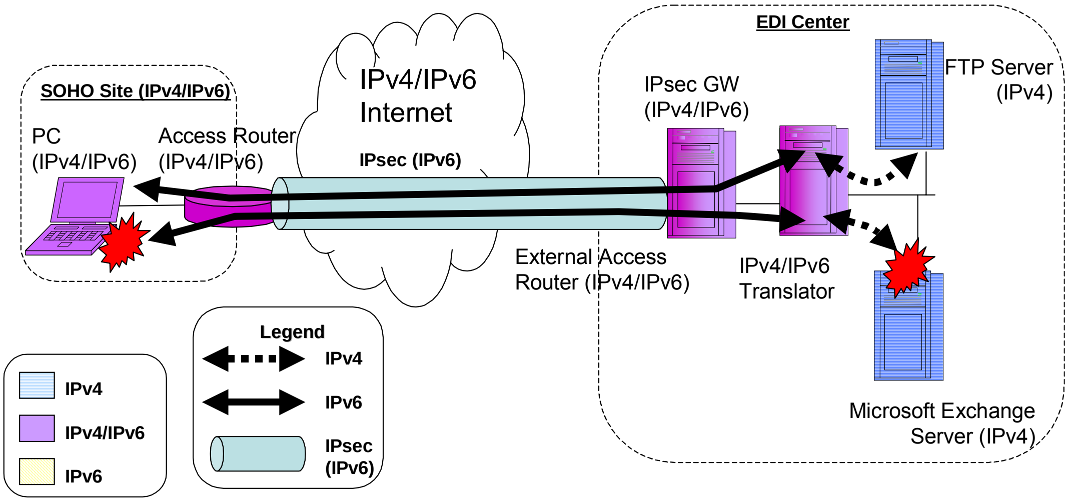


Figure 4.4.2.7: Overview of the Use of Proprietary Business Applications (IPv4/IPv6)

Peer-to-Peer Applications

Here we used IP phones and instant messaging as examples of applications where the characteristics of IPv6 are easy to demonstrate. To determine whether IPv6 communications were possible, we undertook the following tasks during our verifications:

- Simultaneous communications with multiple terminals
- Simultaneous communications between multiple sites
- Simultaneous communications with IPv4 browsing

Results of our verification confirmed that in each situation, use of the application was possible.

When multiple-terminal and multiple-site communications are executed, complex settings are required for the routers and terminals in the same way as for IPv4. With the peer-to-peer applications used on this occasion, special NAT functions were required for holding IP address information in the packet's data segment, and we were not able to achieve multiple-terminal and multiple-site communications using IPv4.

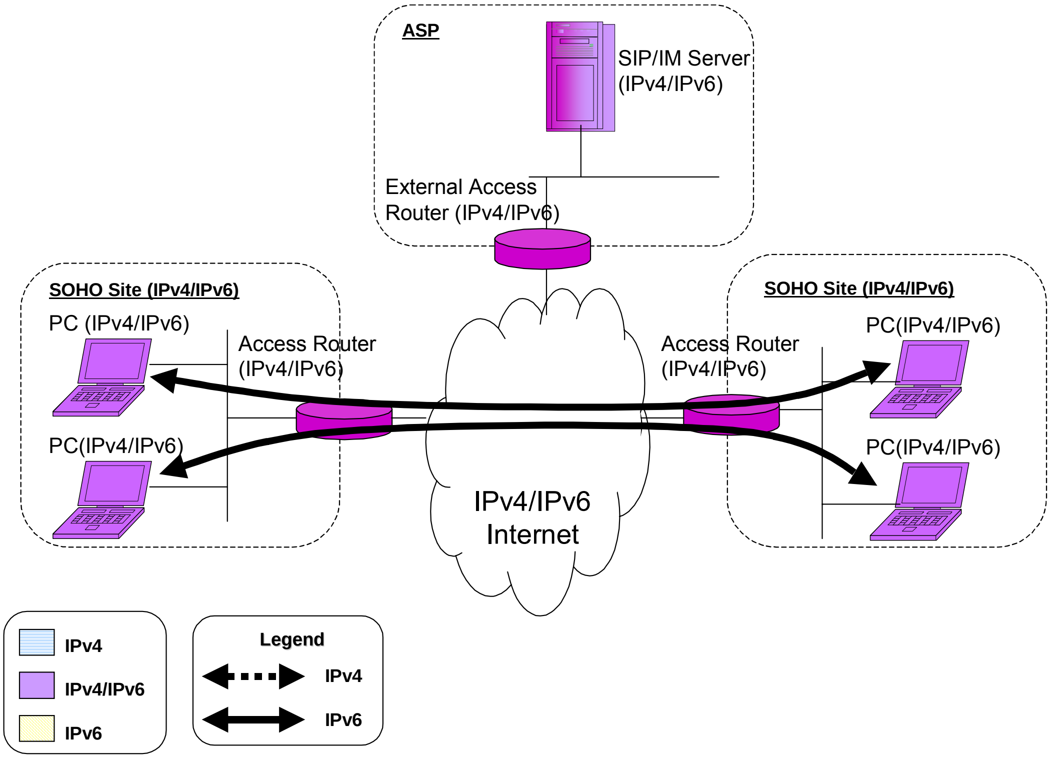


Figure 4.4.2.8: Overview of Multiple Site Simultaneous Communication (IPv6) with Multiple Terminals

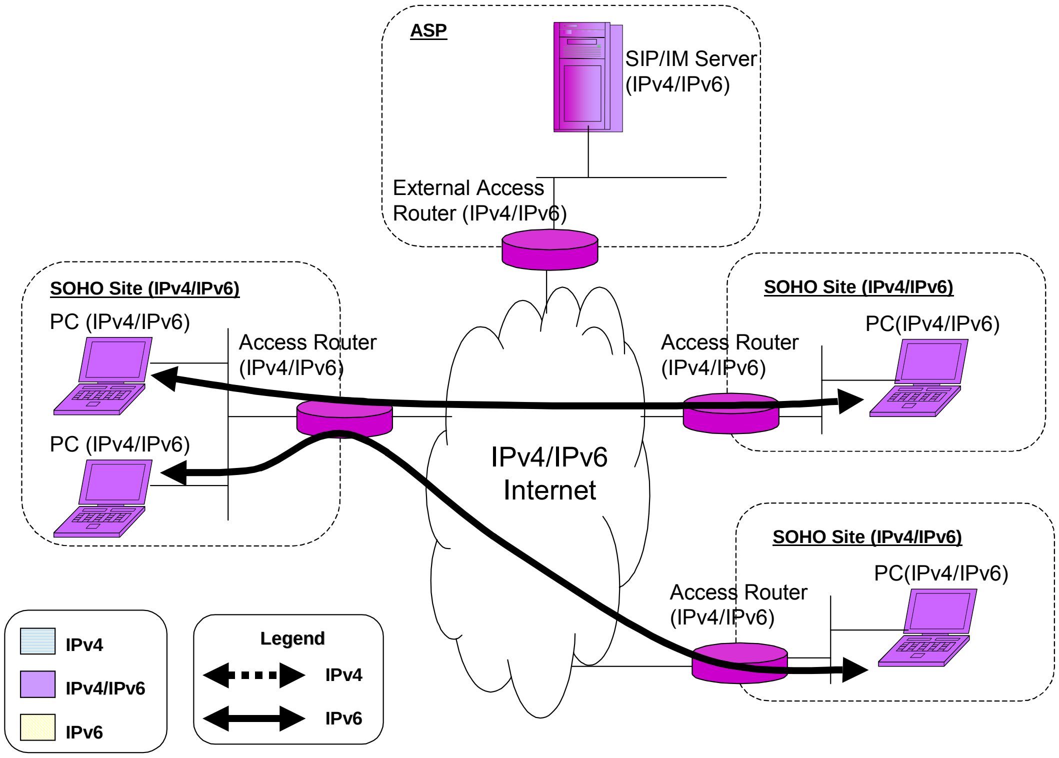


Figure 4.4.2.9: Overview of Simultaneous Communications (IPv6) Between Multiple Sites

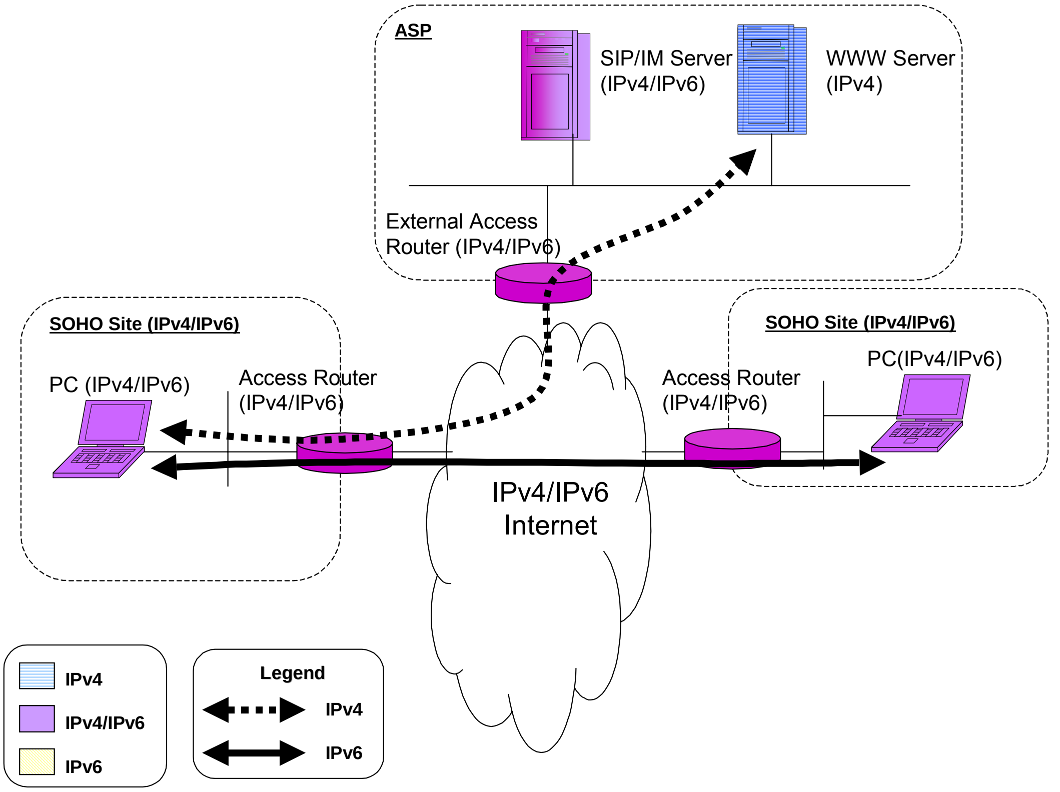


Figure 4.4.2.10: Overview of IPv4 Browsing and Simultaneous Communications (IPv6)

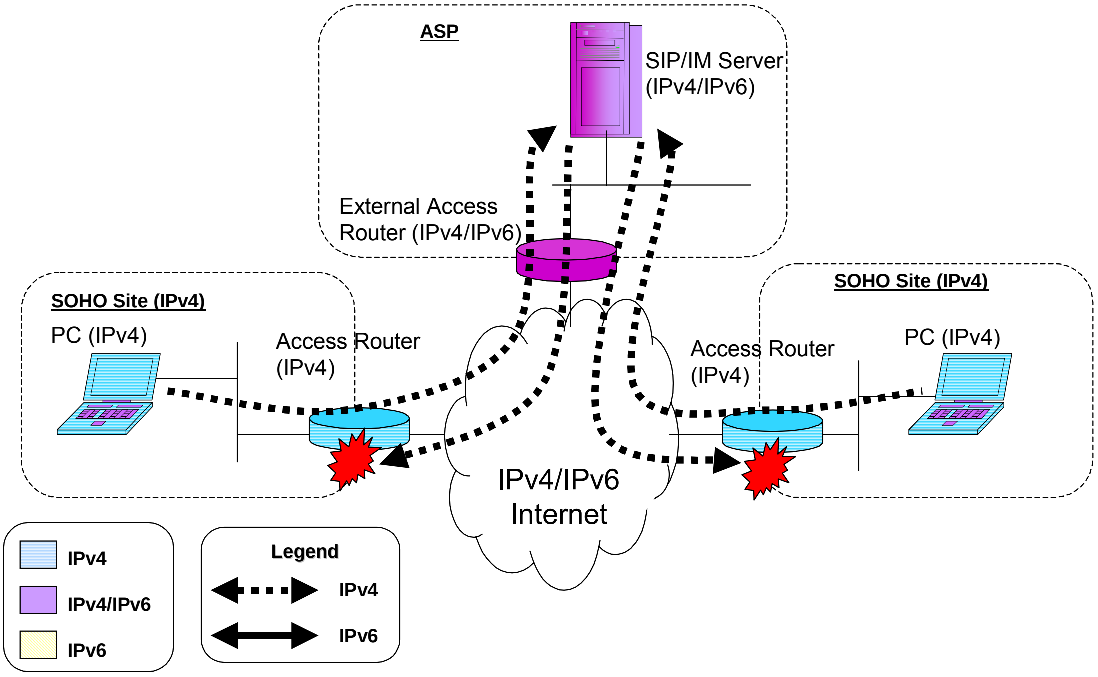


Figure 4.4.2.11: Overview of Peer-to-Peer Communications (IPv4) Using Private IPv4 Addresses

As explained in the Deployment Working Group, an end-to-end environment that can be realized through IPv6 is advantageous for applications performing peer-to-peer applications. Of all the applications we confirmed this time where IPv6 was applied, this was perhaps the most effective application configuration.

Monitoring

For the monitoring, we used Ping to conduct safety checks on the terminals from the EDI Center installed at the SOHO site. In IPv4, the internal network is converted by NAT, so to monitor the internal terminals, complex settings were required for the routers. However, by using IPv6 global addresses, we were able to conduct the monitoring with ease. We believe that an IPv6 end-to-end environment is effective for monitoring and managing the internal network as we did on this occasion.

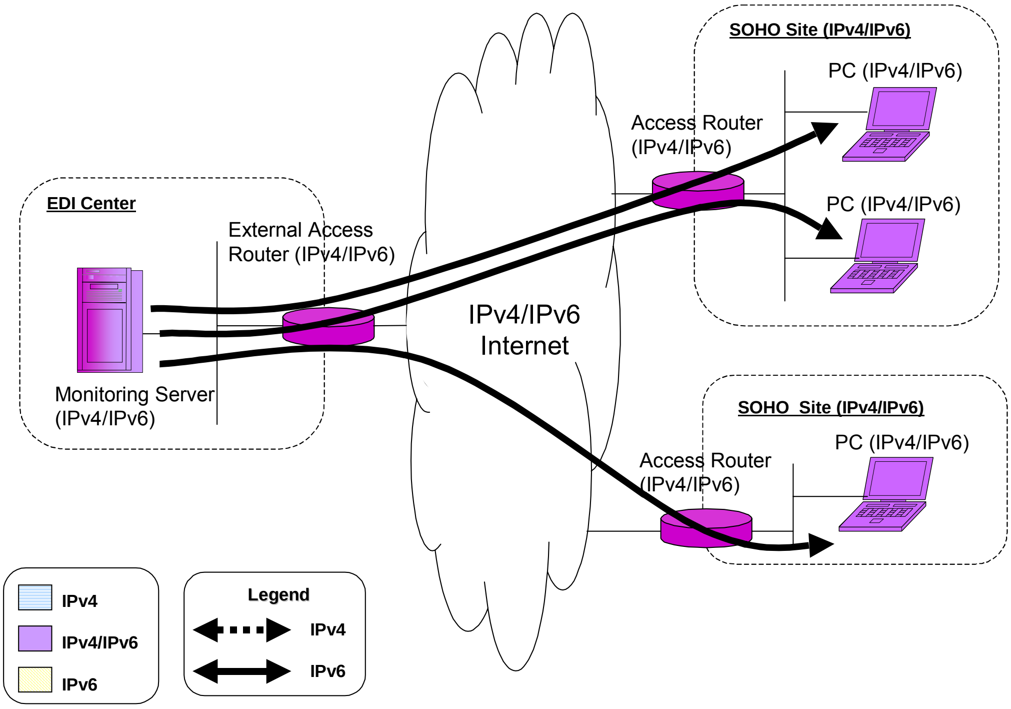


Figure 4.4.2.12: Overview of Remote Monitoring (IPv6)

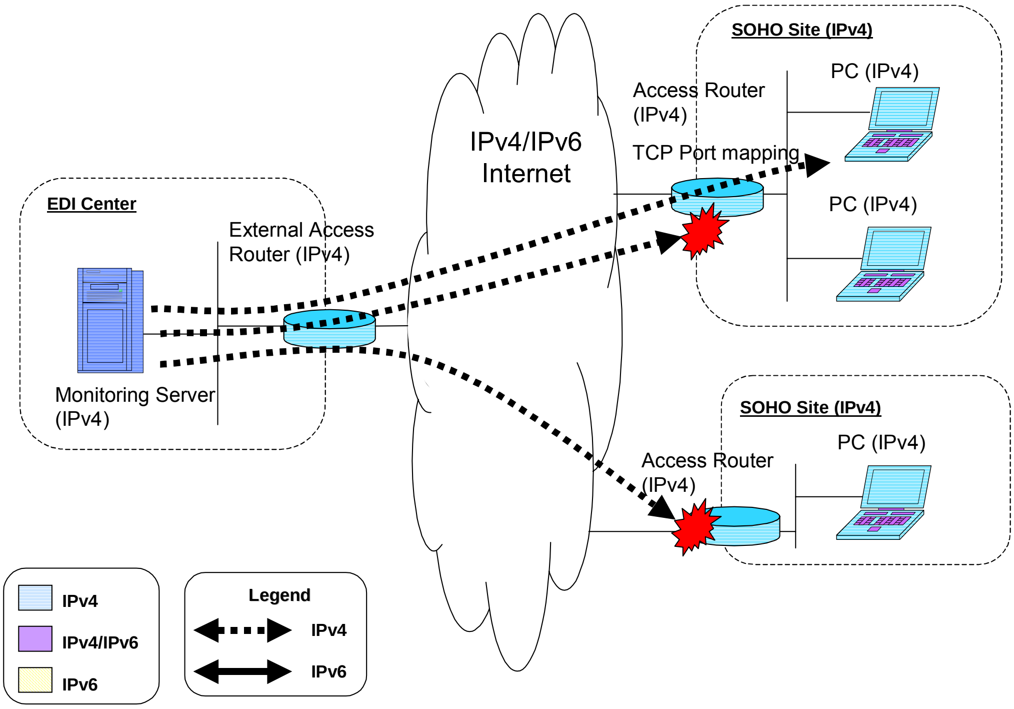


Figure 4.4.2.13: Overview of Remote Monitoring (IPv4)

4.4.3 Other Verifications

Multihome

The Deployment Working Group briefly touched on the possibilities of multihome in a SOHO site. We built a configuration of a multihome at the SOHO site and verified the following two aspects:

- The combination of IPv4 and IPv6 lines
- The combination of two IPv6 lines

For the IPv4 and IPv6 combination, we hypothesized a model where an additional line using an IPv6 environment for IP phones was used in addition to an existing IPv4 line. While ordinary Web browsing was being conducted at the same terminal, we made telephone calls using an IP phone and confirmed that this function could be used without encountering any problems. This type of configuration keeps the impact on an IPv4 system at a low level and can be used for deployment IPv6, so it can be considered effective for the actual deployment of IPv6.

In the second case, where two IPv6 lines were laid, we checked the redundancy of the system. We configured communications using different prefixes set for the respective lines and examined the condition of communications when one of the routers went down assigning multiple prefixes for the same terminal. The line changeover took place when prefix advertisement from the router expired. Consequently, it took time to carry out the procedure, but we were able to confirm redundancy. For the actual application, a function to shorten the down time and a means of suppressing prefix advertisement is required when the line is down. However, we believe this is an effective configuration.

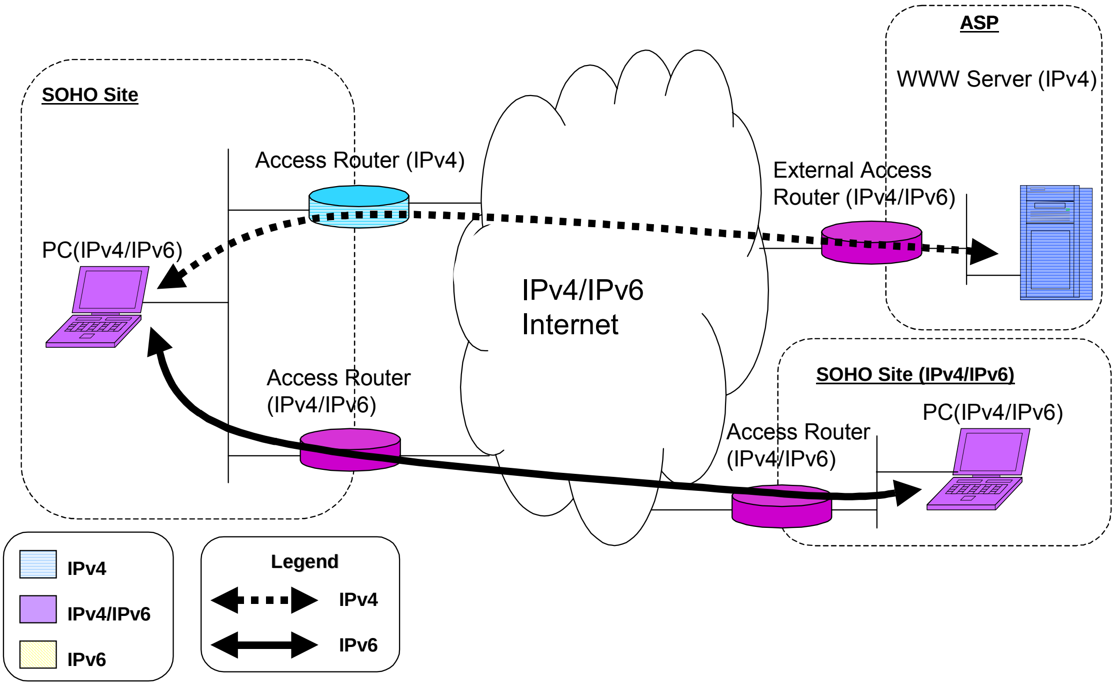


Figure 4.4.3.1: Multihome Overview (IPv4 and IPv6)

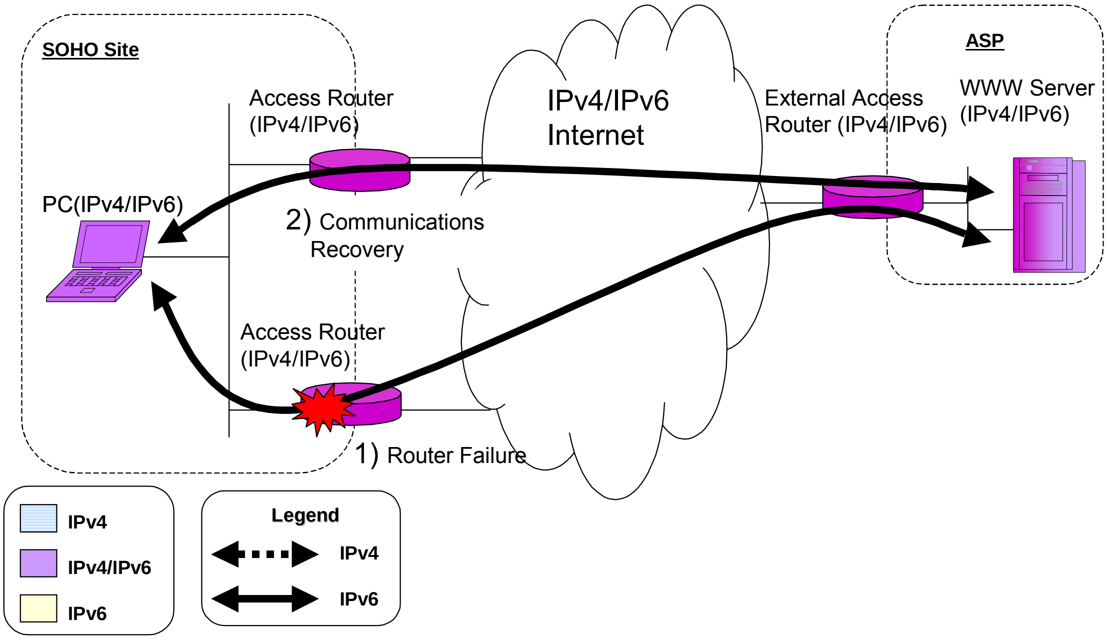


Figure 4.4.3.2: Multihome Overview (two lines: IPv4/IPv6)

4.4.4 IPv6 Deployment Guidelines (SOHO Segment) of the IPv6 Promotion Council

A comparison of areas examined by the Deployment WG Guidelines during the IPv6 deployment phase and verification details verified in Part 2 are shown in the table below.

Overall System

Table 4.4.4.1: A Comparison of the Deployment WG Guidelines and Part 2 (the Overall System)

Description	Deployment WG Guidelines	This Model
Access line	· IPv4 native and IPv6 tunnel · IPv4/IPv6 native · ADSL/FTTH	· IPv4/IPv6 native · ADSL
Access router	· Global IPv6 address (1) (DHCP-PD, Static settings) · Global IPv4 address (1) · Internal address: global IPv6 address (/64) · Internal address: private IPv4 address · Address conversion function · DNS proxy (over IPv4)	· Global IPv6 address (1) (Static settings) · Global IPv4 address (1) · Internal address: global IPv6 address (/64) · Internal Address: private IPv4 address · Address conversion function · DNS proxy (over IPv4)
Center	Generally the existing IPv4	Conversion to dual stack OS depending on the purpose; use of a proxy or translator
Terminal	Using OS that supports IPv6 · Global IPv6 address · Link-Local IPv6 address · Private IPv4 address	Using OS that supports IPv6 · Global IPv6 address · Link-Local IPv6 address · Private IPv4 address

Network

Table 4.4.4.2: A Comparison of the Deployment WG Guidelines and Part 2 (Network)

Description	Deployment WG Guidelines	Part 2
Link used	· Tunnel from router or terminal · Dual stack	· Dual stack (including multihome)
IP Address used in LAN	· Single dual stack /64	Single dual stack /64 (two dual stack /64 in a multihome environment)
IP Address distribution from ISP to user	· Static · Auto allocation (using DHCP PD)	· Static
IP Address distribution to LAN terminals (plug	RS/RA	RS/RA

and play)		
DNS settings for LAN terminals	Using IPv4 (DNS proxy)	Using IPv4 (DNS proxy)

Applications

Table 4.4.4.3: A Comparison of the Deployment WG Guidelines and Part 2 (Applications)

Description	Deployment WG Guidelines	Part 2
Web browsing	· IPv4 access (special server is IPv6-enabled) · Dual stack access	· Dual stack access
Mail	· IPv4 access · IPv4 access (client/server) · IPv6 access (peer-to-peer)	· IPv4 access
Business applications (including Web-based)	· IPv4 access · Dual stack access	· IPv6 access (Outlook, Web access)
Business applications (proprietary application)	· IPv4 access · IPv6 access	· IPv6 access (Outlook, FTP)
Peer-to-peer	· IPv6 access	· IPv6 access
Maintenance	· IPv6 access	· IPv6 access

Security

Table 4.4.4.4: A Comparison of the Deployment WG Guidelines and Part 2 (Security)

Description	Deployment WG Guidelines	Part 2
Encryption	IPsec between gateways, Peer-to-peer IPsec	Peer-to-peer IPsec
Protection against unauthorized access	· IPv4 PFW (GW for IPv6)	· IPv4 PFW (GW for IPv6)

4.5 Evaluation

In this section, we evaluate results achieved by introducing IPv6 to the pre-IPv6 deployment model case detailed in Chapter 4.3 through the migration of each application.

4.5.1 Evaluation from a Building Standpoint

From the perspective of the systems integrator and persons responsible for the IT section of the enterprise, the key issue in construction of the system is to determine whether there are differences in the construction operations of IPv4 and IPv6 by comparing the two. On this occasion, we constructed the IPv6 system modeling it on the IPv4 system, and we did not find significant differences from IPv4 in either the method of building it or the amount of work involved. For the initial deployment of IPv6, the system requires sharing the same environment as IPv4. If the system is being newly constructed, IPv6 can be introduced together with IPv4 construction, so IPv6 introduction does not necessarily mean an increase in operations. Taking into account IPv6's auto-configuration function and less restricted addressing, it is possible that operations may actually become easier to perform than with IPv4 once the system is converted to a wholly IPv6 environment.

However, there are still several issues to consider when we take into consideration the migration process that includes the various applications as well as configuration for use. Specifically, caution must be exercised in the following areas:

- Level of IPv6 support of the system to be used
- Compatibility between different systems (IPsec connectivity, SIP communications, etc.)

These problems can be avoided through careful study at the system design stage.

Furthermore, the system of the communications center that communicates with the SOHO must be more carefully designed, since there are many choices in methods of IPv6 support. For example, choices include the following:

- Making the server support IPv6 directly
- IPv6 support using a translator
- IPv6 support using ALG

On this occasion, we trialed a number of methods of enabling IPv6 support but did not find differences in performance in their use when IPv6 support was possible. There are various characteristics, so it is necessary to select a method after evaluating a number of its features, such as level of impact on server operation, cost, and redundancy.

As a general comment, a number of IPv6-specific terms are encountered relating to IPv6 settings, such as RA, prefix delegation, and DHCPv6. The IPv6 address format also differs from IPv4 and requires getting used to. Therefore, it may be necessary for the systems integrator who is considering the deployment of IPv6 to acquire a minimum basic knowledge of IPv6.

4.5.2 Evaluation from an Operator Standpoint

There are no differences in operational features between IPv6 and IPv4. Therefore, it is necessary to conduct the same operations for IPv6 as were conducted for IPv4, such as monitoring, troubleshooting, and back up.

Since functions that enhance operability and redundancy, such as the use of automatic addressing configuration and multiple prefixes, are well developed in the IPv6 system, it is possible that a network system with greater operability than IPv4 can be constructed. To verify this model system, we built a multihomed network system, and by using both prefixes for each line at the terminals, we were able to test the detouring when there was failure in the routers and to confirm the movement. Using the IPv6 network system in this way, we are able to confirm its high reliability as a network system.

On the other hand, from the operator’s point of view, there seem to be some cases where the automatic settings of the terminal actually result in loss of manageability. For example, when the IPv6 address is automatically set, the end user does not know the address of his or her terminal, and consequently, this complicates monitoring, operation, and troubleshooting.

To increase the efficiency of monitoring, we tried automatic registration of IP addresses of terminals using dynamic DNS functions. The operation of an IPv6 network, with its combined automatic terminal settings and automatic operation functions, allows the possibility that its operability can be enhanced beyond the operation of a network using IPv4.

However, to make a generalization, the operating functions of IPv6 are not yet fully developed. For example, even on devices where IPv6 functions are supported, there are many operating functions that cannot be used with IPv6 access, such as use of SNMP functions, device settings, and Web access. In the future, improvements can be expected in the operational functions in IPv6 which will make them applicable on a wide scale.

4.5.3 Evaluation from a User Standpoint

The terminals mainly used by the assumed users of SOHO are currently PCs. In the environment in which the model case was constructed, to conduct evaluations into ease of use and other areas, we used a PC running Windows XP. As a result, we were able to use IPv6 for applications used in IPv4, such as Web browsing and IP phone, with almost no obvious awareness of the use of IPV6. From the end user's perspective, there is almost no difference between IPv4 and IPv6.

However, there are still applications (such as DNS query, Outlook, virus checker) where IPv6 support is not yet available, so under the current circumstances, IPv4 access is still needed.

4.5.4 Evaluation of Deployment Costs

Windows XP, the OS used in a large number of PCs, supports IPv6. Though there is still a large number of low-end routers that do not support IPv6, the number of SOHO-class routers supporting IPv6 is increasing. We constructed an environment based on the model case, and in terms of equipment, the configuration was exactly the same as the existing construction for IPv4 and involved simply adding settings; therefore, there was nothing in particular that needed to be added. The SOHO system is relatively simple and requires only a few kinds of equipment, such as PCs and routers. The cost of equipment in introducing IPv6 to an environment like SOHO is therefore considered to be very small. In addition, operations for configuring settings can be carried out in the same manner as in ordinary IPv4 construction. While there are some costs involved in executing these operations, they can be minimized.

The most significant cost that may be incurred in SOHO appears to be for applications that support IPv6. Costs are incurred particularly for the development and distribution of proprietary business applications that need to support IPv6. However, recent business applications used on networks are being converted to Web services to cut costs for client management, and the actual extent of the impact of proprietary applications on costs for IPv6 may therefore be minor.

4.5.5 Tips

(1) Multihome

Using a multihomed configuration combining an IPv4 line and router and a dual stack line and router, we were able to confirm that use of both IPv4 and IPv6 applications respectively were possible. In a multihomed configuration that uses a connection mediated by an IPv4 dedicated access router and a connection mediated by an IPv4/IPv6 dual stack access router, even if a failure specific to IPv6 occurs, its effects can be minimized by using the IPv4 dedicated route. Furthermore, when considered as a method of migration to IPv6, this configuration presents relatively little migration risk, since IPv6 is introduced as an addition to an existing IPv4 system.

(2) Dynamic DNS

We set the monitoring system to use dynamic DNS functions in the terminals to be monitored. Using dynamic DNS functions, we confirmed that monitoring and remote maintenance could be performed by specifying the FQDN for the target terminals, even when the network connecting the terminal and the IPv6 address of the terminals changed. We believe that in actual SOHO networks, dynamic DNS functions can easily be used to support the moving and the changing of addresses of terminals to be monitored.

4.6 Future Issues

This section discusses issues that became apparent when we actually introduced IPv6 to the network model.

4.6.1 Network

Management of Global Address Prefixes

In our verifications, we did not formulate any particular guidelines in regard to the way in which global address prefixes should be distributed to which segment. However, it is necessary to consider the handling of prefixes when performing various operations using addresses as identifiers, such as securing communication quality that takes into consideration the user terminals, servers and users, and when executing load distribution and multihomed configuration.

Additional Information regarding Address Distribution to Terminals

During our verifications, we used RS/RA for the distribution of IPv6 addresses to terminals, but we were not able to distribute the DNS information required for the use of general applications. Therefore, for DNS address resolution at the terminals, we used IPv4 DNS server information obtained from IPv4 DHCP. A future issue to consider is how DNS information will be obtained in an environment where only IPv6 addresses will be automatically assigned.

4.6.2 Applications

Use of Applications with IPv6

In our verifications, we checked whether or not existing IPv4 applications could be used with an IPv6 terminal. At that time, we confirmed that certain applications could not be performed with an IPv6 terminal. For an application to be usable even with an IPv6 terminal, both the protocol used and the application itself must support IPv6. Furthermore, even when the previously mentioned conditions do not support IPv6, it may be possible to use the applications with an IPv6 terminal using an address conversion function such as a Web proxy or an IPv4/IPv6 translator. In such cases, however, verifications to confirm whether they can be used must be conducted in a test environment beforehand.

4.6.3 Security

IPv6 Support for Security Software

To establish security, we verified gateway packet filters and VPN between terminals in our verifications. However, in the actual application, security check functions corresponding to the applications used are necessary. For example, general applications, such as Web browsing and mail, require a security check function (for viruses) that supports IPv6. Therefore, for applications where security check functions do not support IPv6, continued use of the existing IPv4 is advisable.

Automatic Security Settings

For this verification, we performed manual settings to establish security. However, for use in an actual system, intricate security policy design and device configuration will need to be performed automatically.

VPN between Terminals

In this verification, we conducted end-to-end communications between terminals where a VPN was established using IPsec. During that time, we confirmed instances where security could not be fully established with some of the applications used. For example, in the case of peer-to-peer applications that used an SIP server, data between the terminals where VPN had been established was encrypted. However, data from the SIP server to each terminal was not encrypted. Therefore, even when a VPN is established in end-to-end communication, for applications where there is communication with third parties, establishing a VPN between all related communication parties to ensure security is advisable.

5. Guideline for Home Segment

5.1 Overview

This chapter shows guidelines for IPv6 deployment at a private home. In Part 2, a model case environment for a private home that is in the process of deployment is actually created. The sections describe solutions necessary for migrating from an environment with only IPv4 equipment to a mixed environment that uses both IPv4 and IPv6 equipment. The advantages and challenges to implementing such an environment are also described.

Since it is generally assumed that a network administrator does not fit in the home segment, Part 2 is intended for vendors and service providers who develop IPv6 equipment for home use. The descriptions include a wide variety of general descriptions explaining deployment scenarios or deployment techniques for the home segment.

5.2 Typical Deployment Scenarios for Home Networks

Migration scenarios for home networks are defined in the deployment guideline developed by the IPv6 Promotion Council DP-WG (hereinafter referred to as the "Deployment WG Guidelines"). The deployment scenarios were selected by considering the following points:

- The number of IPv6-compatible networks and amount of IPv6-compatible PC equipment currently available in the market is gradually increasing, but their functions are not fully known to users.
- Demand for network-compatible home appliances (nPC) is likely to increase, and they are assumed to be single-stack in terms of machine resource and cost.

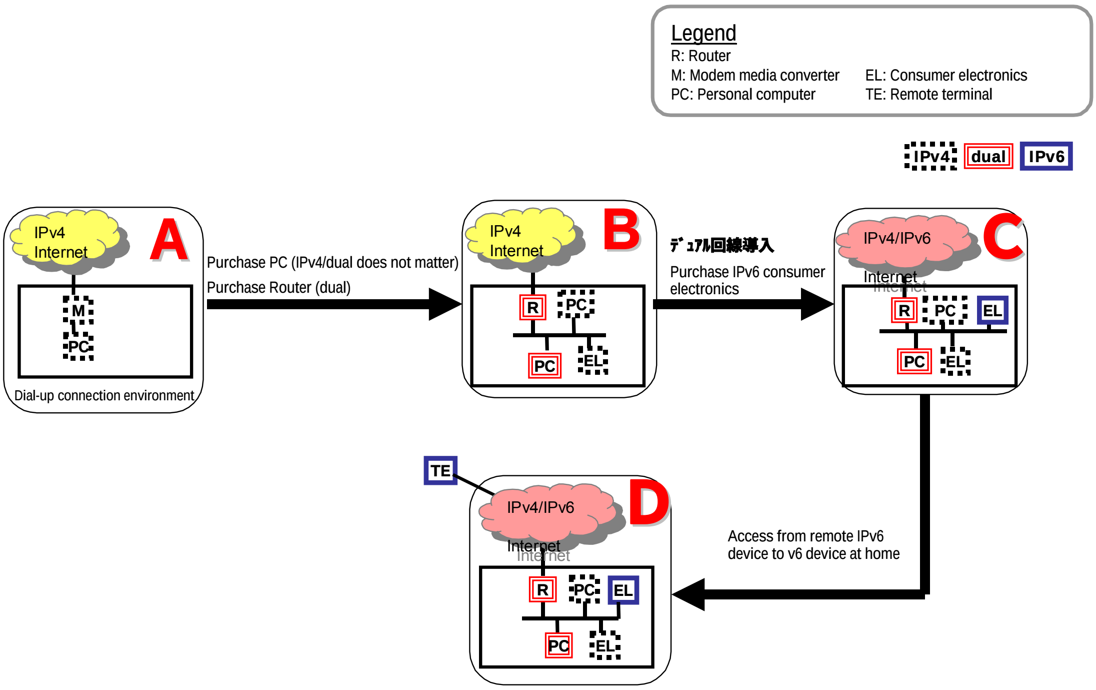


Figure 5.2-1: Deployment Scenario

5.2.1 Prior to IPv6 Deployment

Figure 5.2.1.1 shows a typical home network configuration before IPv6 deployment.

This model corresponds to Model A of the deployment scenario. It includes a single personal computer (or the like) in a private home and the whole network environment including networks and the boundary between the home and other networks (including a modem using a bridge connection) is compatible only with IPv4.

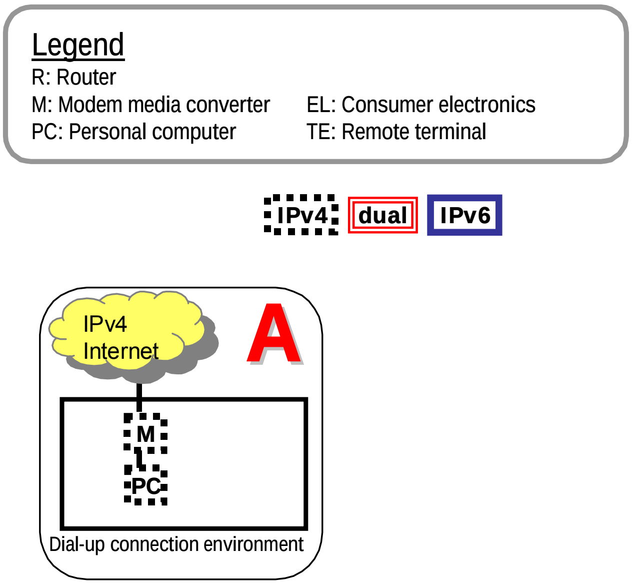


Figure 5.2.1.1: Current Model

5.2.2 IPv6 Deployment Step 1

The configuration of this model is shown in Figure 5.2.2.1.

This model corresponds to Model B of the deployment scenario. Equipment that users buy at a store including a router and a PC are dual-stack compatible, but they are still using IPv4 to connect to the Internet. Even the dual-stack compatible equipment is used only as IPv4 equipment.

Legend
R: Router
M: Modem media converter
PC: Personal computer
EL: Consumer electronics
TE: Remote terminal

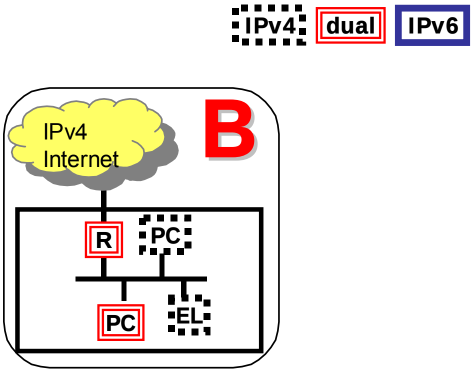


Figure 5.2.2.1: Deployment Model 1

5.2.3 IPv6 Deployment Step 2-1

The configuration of this model is shown in Figure 5.2.3.1.

This model corresponds to Model C of the deployment scenario. With this model, it is expected that the next step is to install digital consumer appliances in a private home. In a situation where digital consumer electronics are sold in a general store, in terms of cost and machine resource there are significant obstacles to make the appliances dual-stack compatible. Therefore, eventually the appliances may only be compatible with IPv6. A connection to the Internet will be converted to IPv4/v6-compatible equipment along with the installation of IPv6-compatible equipment.

There is a lack of easy-to-use input/confirmation setup functions for most electronic home appliances (remote control units, liquid crystal displays capable of displaying several lines of text, etc.). Therefore, intercommunication between existing IPv4 equipment or dual use equipment and IPv6 equipment will be necessary, which is the difference between Step 1 and Step 2-1.

Legend

R: Router

M: Modem media converter EL: Consumer electronics

PC: Personal computer TE: Remote terminal

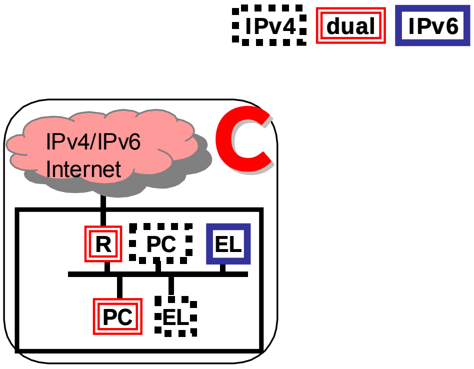


Figure 5.2.3.1: Deployment Model 2-1

5.2.4 IPv6 Deployment Step 2-2

The configuration of this model is shown in Figure 5.2.4.1.

This model corresponds to Model D in the deployment scenario. The configuration inside the home is the same as Section 5.2.3 but the difference is that there is access from outside the home to inside the home. If the demand for IPv6 increases and a service using mobile equipment is launched (providing a means to communicate between IPv6 equipment inside the home and IPv6 equipment outside the home), the network environment may be migrated to this model.

Access from outside the home to inside the home is via end-to-end communication supported by varieties of IP addresses featuring IPv6. This model was selected because this is likely to be the mainstream for mixed IPv4 and v6 environments.

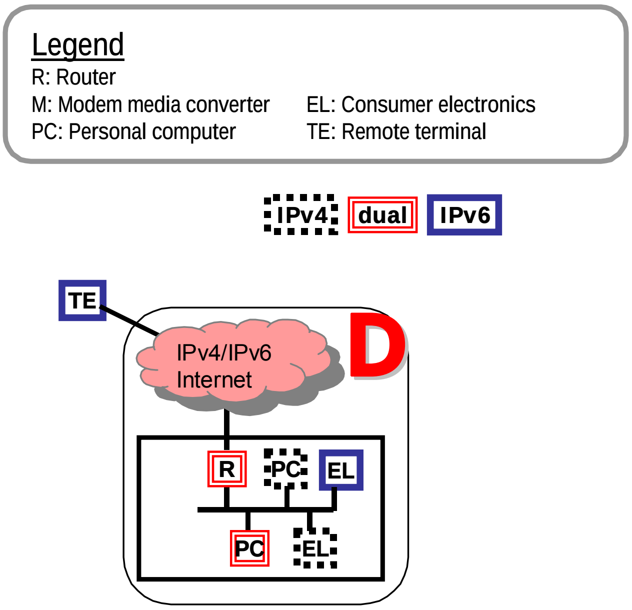


Figure 5.2.4.1: Deployment Model 2-2

5.2.5 IPv6 Deployment Policy

This section will describe policies for IPv6 deployment introduced in the Section 5.2.4 where a model case is discussed. As described in Section 5.1 since there are no network administrators in the home segment, this section will analyze the features of the domestic segment and outline policies for network device vendors and vendors of home devices.

(1) Simplification of device information management

As stated earlier, there are no network administrators in the domestic segment. Network devices, PCs, each home uses a personalized assortment of digital consumer appliances that have a variety of operating statuses.

In this type of environment, it would be virtually impossible to require a home user to manage home appliances and cope with IPv6 addresses. A procedure that simplifies management of devices in the home is therefore in order.

(2) Using existing IPv4 devices

Now that always-on broadband services is becoming more common, IPv4 networks have started to enter the home environment. AV devices and game consoles that can only use IPv4 have also found favor in many homes.

Migration to IPv6 would be delayed if the introduction of IPv6 devices would prevent use of existing IPv4 devices. It is therefore essential that an environment be built that enables the coexistence of incompatible IPv4 devices with IPv6 devices.

(3) Ensuring security of IPv4/IPv6 devices

Communications with external networks in an IPv4 environment is normally implemented using NAT and security is assured through the use of routers with built-in firewalls. In an IPv6 environment, in addition to firewalls, devices are assigned a global address and consequently are able to maintain their own security (IPsec, etc.) during communication with outside networks. Thus, in a mixed IPv4 and IPv6 environment, the coexistence of communications via firewalls and end-to-end communications is an essential condition in the migration process. Alternative security measures must be introduced when cost considerations, equipment resource problems make encrypted communications (IPSec) impractical even for IPv6 devices.

5.3 Specific Cases

As shown in the deployment scenario at the beginning of Section 5.2, there is almost no difficulty with deployment in Models A and B since they are not intended to use IPv6 at this stage. Model C is considered to be the same as Model D except that access from outside the home occurs. In Part 2, an environment where IPv4 and IPv6 coexist is actually created based on Model D (Section 5.2.4), which is an in-between model for migrating to IPv6 in the home. In addition, troubleshooting for issues based on the policies described in Section 5.2.5 are reviewed and evaluated.

The Part 2 describes the model created in these sections.

5.3.1 Model case

The existing IPv4 equipment and a Windows PC that is IPv4/v6 dual-stack compatible will be connected to the network. A network camera connected to the network serves as an IPv6-compatible digital consumer appliance.

For controlling IPv6 digital consumer electronics from existing IPv4 equipment or IPv4/v6 equipment, a controller unit (hereinafter called the "translator") is used that implements functions for collecting and displaying equipment information using a protocol conversion and NIQ/NIR, ICMPv6 ECHO.

IPv4/v6 compatible routers and external networks are provided to implement an environment in which access from inside to outside the home using an IPv6-compatible PC is included.

Network configuration

The network configuration of this model is shown below.

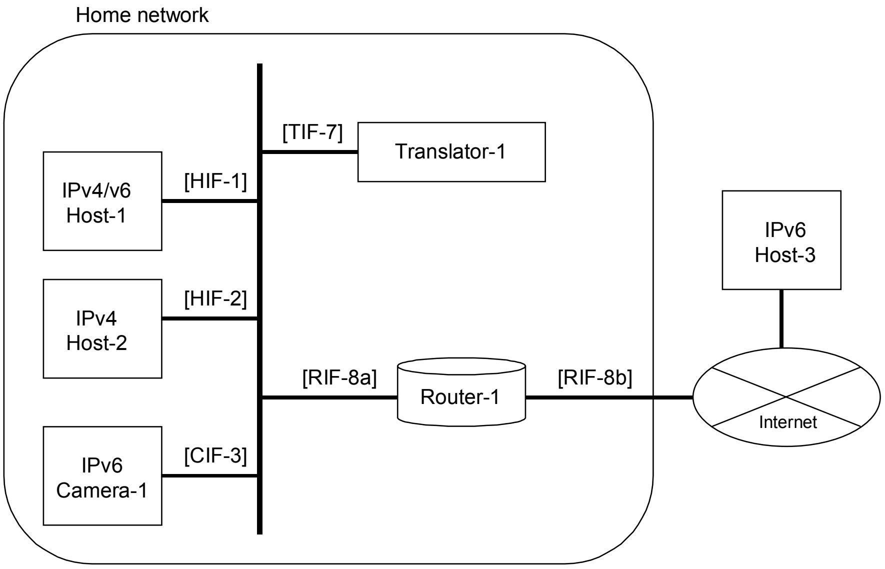


Figure 5.3.1.1: Network Configuration

The specific configuration of equipment is as follows.

Table 5.3.1.1: Equipment Configuration Table

No.	Equipment	Spec / OS	NIQ/NIR	ICMPv6 ECHO	IF(NIC)	IPv4 address
						IPv6 address
1	IPv6 Host-1	Windows XP	Not supported	Supported	HIF-1	Auto configured by DHCP
						Auto configured by autoconf
2	IPv4 Host-2	Windows XP	Not supported	Not supported	HIF-2	Auto configured by DHCP
3	Camera-1	KX-HCM130 / -	Supported	Supported	CIF-3	
						Auto configured by autoconf
7	Translator-1	PSS-TR-001 / NetBSD1.6	Supported	Supported	TIF-7	10.4.0.5
						Auto configured by autoconf
8	Router-1	RT56v / -	Not supported	Supported	RIF-8a	10.4.0.1
						2001:db8:4000::1
					RIF-8b	Auto configured by PPP IPCP
						Auto configured by PPP IPv6

Applications

This section describes each function built in this model.

(1) Collection/registration/reference functions for home equipment list information (name resolution inside the home)

The translator periodically sends “NIQ”, “ICMPv6 ECHO”. If the equipment connected to the network inside the home is compatible with those protocols (standardization of the NIQ protocol is now under review), it returns its information as a response and the translator saves the information.

The applicable information saved in the translator can be made available to other devices as HTML content.

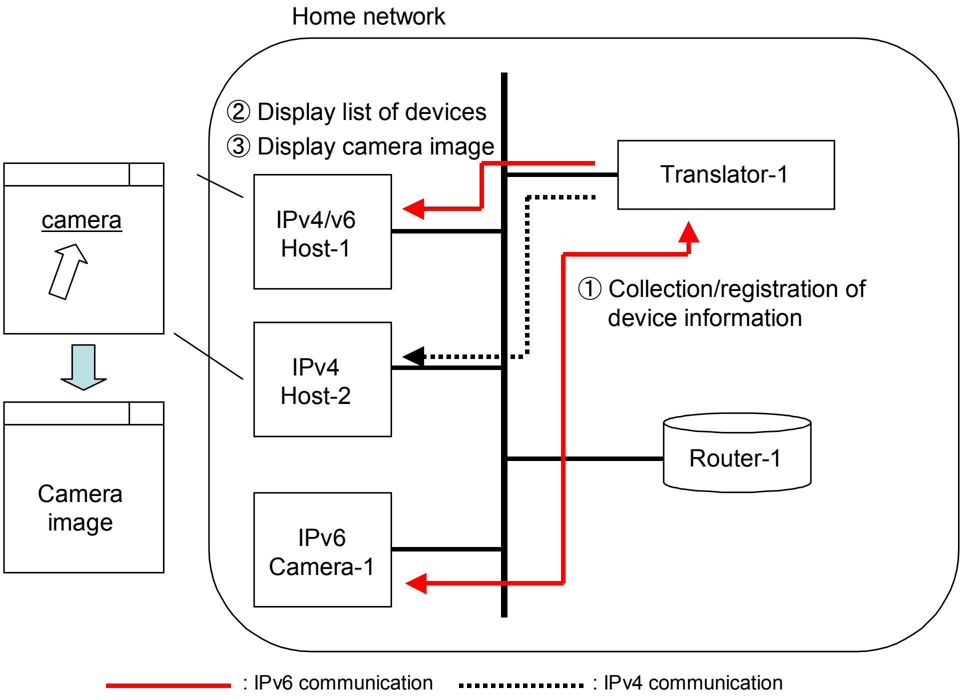
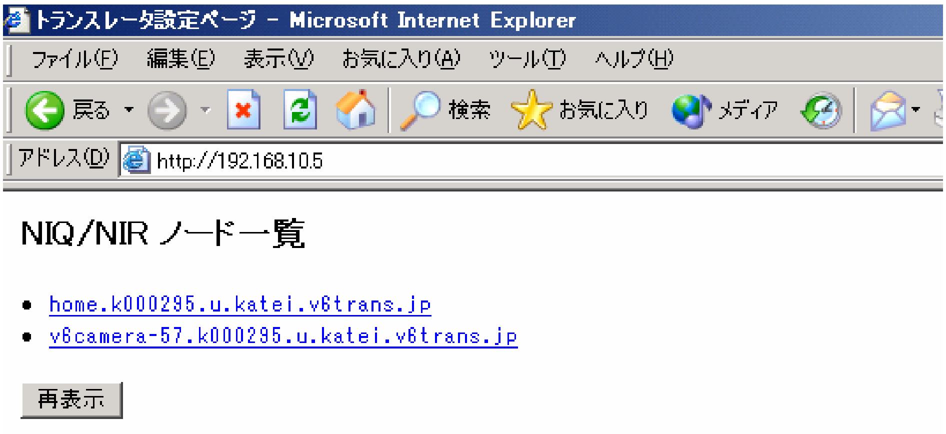


Figure 5.3.1.2: Collection/Registration/Reference Functions for Home Equipment List Information


トランスレータ設定ページ - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
検索
お気に入り
メディア
アドレス(D)

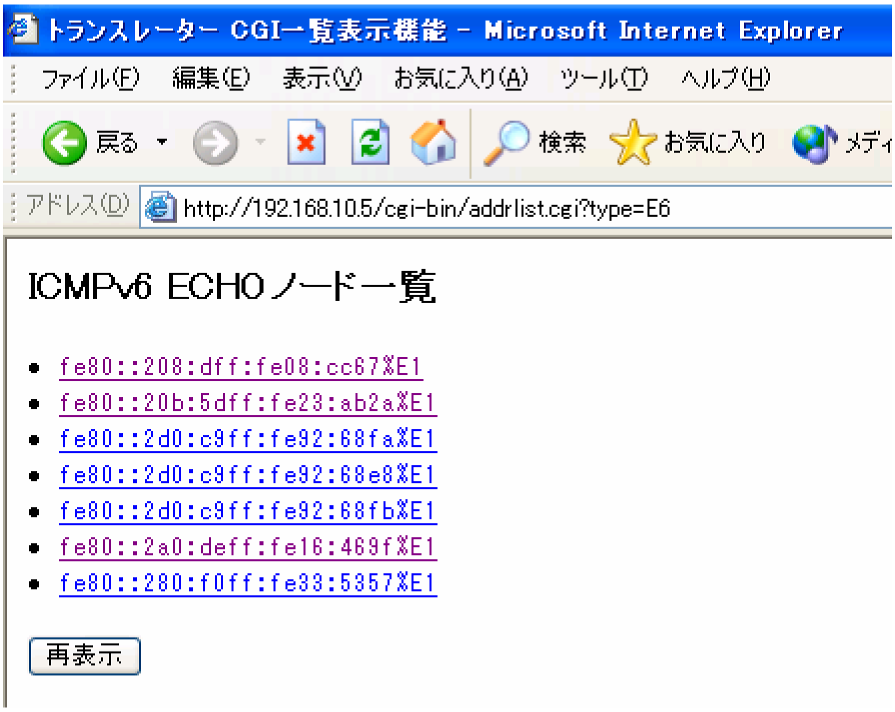
http://192.168.10.5

NIQ/NIR ノード一覧

- home.k000295.u.katei.v6trans.jp
- v6camera-57.k000295.u.katei.v6trans.jp

再表示

Figure 5.3.1.3: Screen Image of Home Equipment List (NIQ/NIR)


トランスレーター CGI一覧表示機能 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
検索
お気に入り
メディ
アドレス(D)

http://192.168.10.5/cgi-bin/addrlist.cgi?type=E6

ICMPv6 ECHO ノード一覧

- fe80::208:dff:fe08:cc67%E1
- fe80::20b:5dff:fe23:ab2a%E1
- fe80::2d0:c9ff:fe92:68fa%E1
- fe80::2d0:c9ff:fe92:68e8%E1
- fe80::2d0:c9ff:fe92:68fb%E1
- fe80::2a0:deff:fe16:469f%E1
- fe80::280:f0ff:fe33:5357%E1

再表示

Figure 5.3.1.4: Screen Image of Home Equipment List (ICMPv6 ECHO)

(2) Auto-registration address function (name resolution outside the home)

The translator has a function to broadcast its IP address and host name automatically to an external server. By sending the pre-configured ID and password simultaneously, the center authenticates them. If the equipment is authenticated, the information sent to the server is registered in the DNS. This function allows users to access the translator by their name from an external environment without registering their address in advance. It also is intended to minimize the number of devices registered with the DNS.

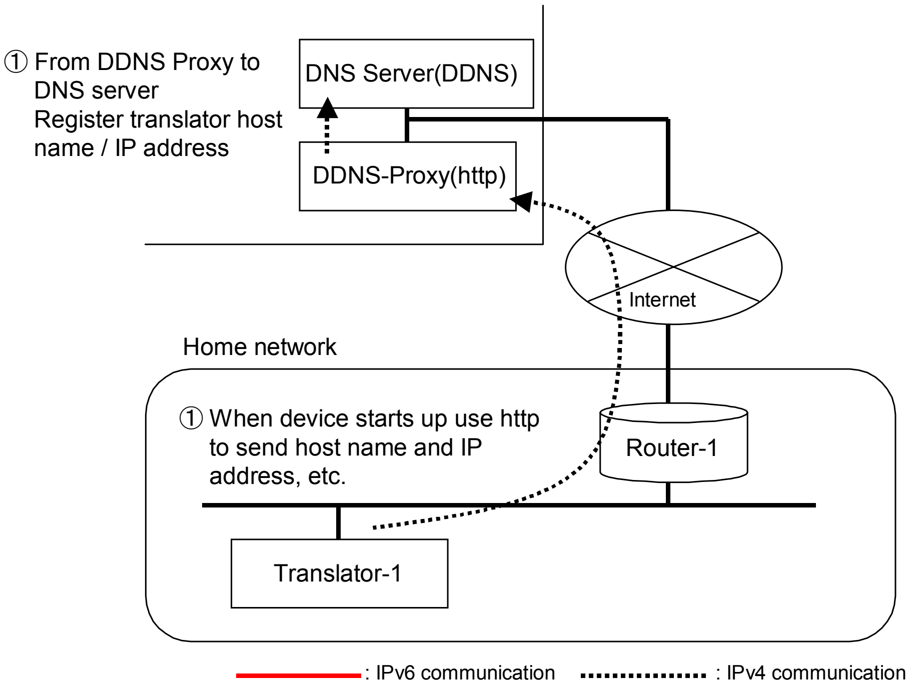

① From DDNS Proxy to DNS server Register translator host name / IP address
DNS Server(DDNS)
DDNS-Proxy(http)
Internet
Home network
① When device starts up use http to send host name and IP address, etc.
Router-1
Translator-1
: IPv6 communication
: IPv4 communication

Figure 5.3.1.5: Auto-registration Address

(3) Security function

IPv6PC and the translator implement IPsec communication; this is accomplished by installing VPN client software (MyNetManager) on a Windows IPv6PC, and installing raccoon on the translator, which runs on NetBSD.

To ensure security of IPv6 equipment not capable of implementing IPsec due to restrictions such as equipment performance or capacity, the equipment is allowed to communicate via the translator only, and the packet is relayed by having the translator communicate via IPsec.

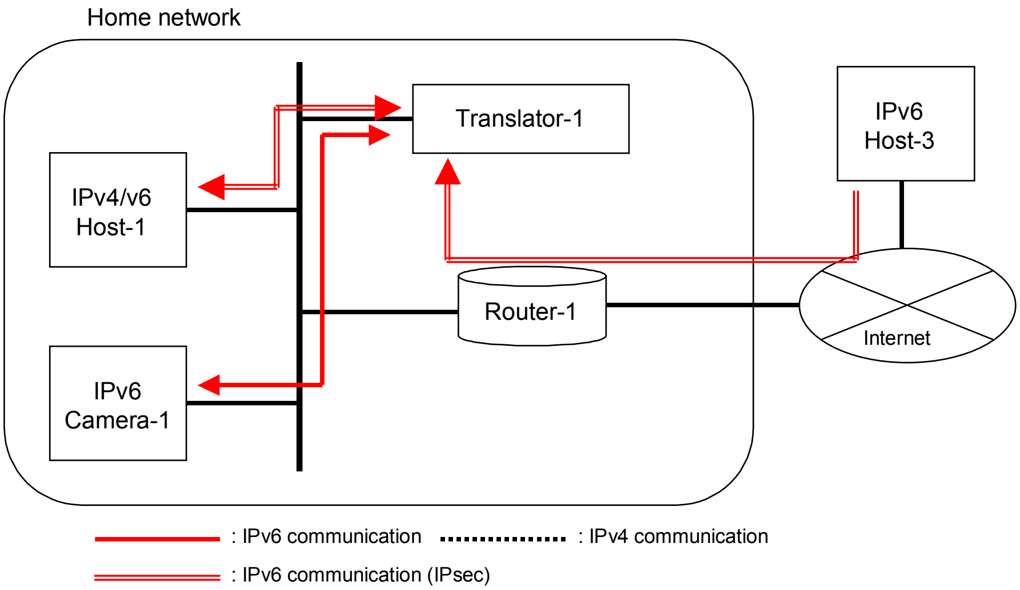


Figure 5.3.1.6: IPsec Proxy Response

(4) Protocol conversion function

Communication between IPv4 equipment and IPv6 equipment using an IP protocol is basically not possible. However, to make it possible, a Bi-Directional-NAT-PT translator is installed to implement interconversion of the protocol.

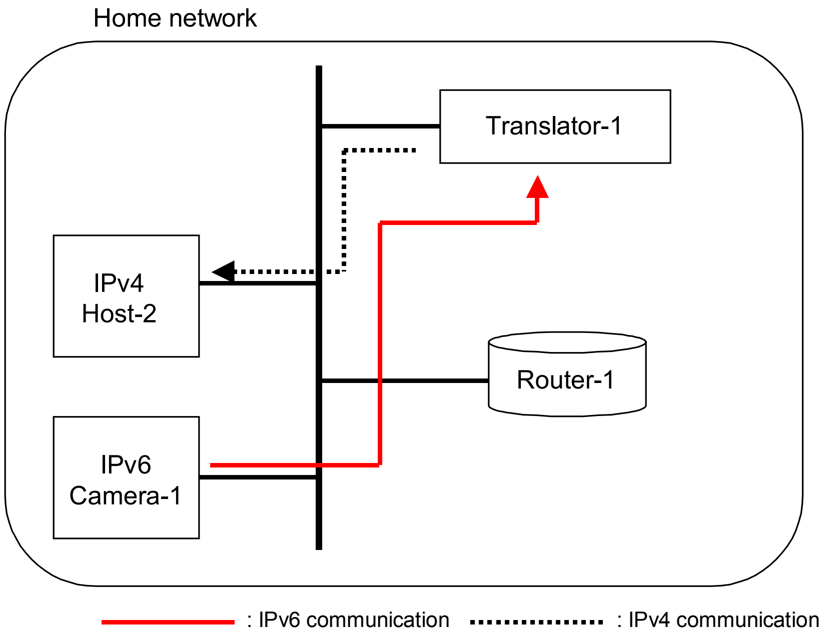


Figure 5.3.1.7: Protocol Conversion

5.3.2 Evaluation

This section evaluates the result of the deployment model that was actually used.

The point of the evaluation was to focus on how much each of the applications was needed, and how simple the operations and configurations were.

(1) Collection/registration/reference functions for home equipment list information (name resolution inside the home)

[Technical evaluation]

The home equipment list was validated using “NIQ/NIR” and “ICMPv6 ECHO” and it was proved that operations in the both systems were successful. However, in the case of ICMPv6 ECHO, the browser was unable to handle IPv6 addresses directly and could not use the collected information, since ICMPv6 ECHO only handles site local address information. In addition, it was not possible to determine to which equipment the information displayed corresponded. On the other hand, in the case of NIQ/NIR, information was fully available since the host name was displayed without suffering restrictions from any function of, for example, a browser.

In cases in which the functions of the home equipment list are to be provided, a method to collect information other than addresses is recommended when considering cases in which the environment (i.e. the OS or browser application) is not fully compatible with IPv6.

[Evaluation by users]

A user survey regarding the home equipment list using NIQ/NIR yielded the following information:

- The function is convenient: 83%
- I will use the function every time: 65%

We confirmed that the configuration of the function that collects equipment information inside the home and enables access via a GUI is simpler than a system to allow users to manage IP addresses directly (displaying the controlling screen of a camera, investigating addresses, describing addresses in a hosts file).

The assumed reasons for the decrease of users using this function every time is because the number includes users who are using the function for the first time and use their favorite functions on their browser after that (we could not directly input IPv6 addresses in the version Internet Explorer we used), thus the decrease is due to problems described in a later chapter.

(2) Auto-registration address function (name resolution outside the home)

(3) Security function

[Technical evaluation]

In cases in which the function to transfer IPsec communication terminated at the translator to other equipment within the same segment is used, plain text is used for communication within the home. However, because there is no problem with usage within the home in terms of packet level security, as a result this function is considered to be effective.

[Evaluations by users]

In this experiment, a camera was installed in the home, but everyone succeeded in accessing the camera outside the home, proving that the registration of the address to the external DNS was successful. However, 62% of people were worried about security at the time of the experiment. We had explained about encryption using IPsec and about other matters related to security in advance, but several factors that were not transparent to users seemed to be the cause of anxiety, such as the effectiveness of security using IPsec communication. It seems that there is also a sense of resistance in disclosing equipment inside the home.

We also asked questions about the decrease in response time on using IPsec.

- Almost no difference between encrypted and non-encrypted systems: 62%
- Encrypted communication seems to be slower: 30%

No one answered that they don’t want to use encrypted communications because encrypted communication is too slow. The response proved that even in a configuration where a general OS (NetBSD) is used, there is no problem with processing speed.

(4) Protocol conversion function

[Technical evaluation]

A “Bi-Directional-NAT-PT” system was used to convert addresses, and by combining with the collect home equipment list function (NIQ/NIR), communication between IPv4 and IPv6 was carried out without changing the equipment configuration, which proved to be effective for managing equipment inside the home.

However, a problem occurred with conversion during communication from outside to inside the home.

[Evaluation by users]

A user survey yielded the following information:

- I think the translator is necessary: 86%
- Using the translator, I can buy equipment without worrying about compatibility: 80%

The response proved that the protocol conversion function is effective.

Enabling access from existing IPv4 equipment to IPv6 equipment removes a psychological barrier for users considering purchasing IPv6 equipment, which proved to be a big factor for promoting deployment.

A user survey yielded the following information about the speed of protocol conversion:

- There is no problem since it is within the allowance: 60%
- A little slow but there was no problem with usage: 30%

The response proved that converting protocols using this software causes almost no problem for communication with an IP camera.

There were several other problems for each of the topics, but from the viewpoint of user and technical evaluations we were able to confirm that there is no problem with the policy for deploying IPv6 described in Section 5.2.5.

- Users purchase dual-stack-compatible equipment including PCs and routers without worrying about compatibility.
- Routers (or equipment including home servers that have similar functionality) support the home equipment list, security and protocol conversion functions.
- Users do purchase digital consumer electronics that are only compatible with IPv6 (some appliances do not support IPsec).
- Owing to the above functions working in the routers, users can use equipment safely from inside and outside the home without worrying about compatibility with IPv4 or IPv6.

The scenario drawn according to Section 5.2 seems to be the mainstream of the home segment.

* 69 users answered the questionnaire (13 respondents only use wireless access from outside the home)

5.3.3 Issues

In this section, we discuss issues that rise to the surface when we actually configure this deployment model.

(1) Collection/registration/reference function of home equipment list information

- Reflection of information to the equipment list

Some people said they feel it takes time to update the list when new equipment is connected or devices are removed. (It currently takes 1 minute.) Update frequency needs to be increased while taking the communication volume into consideration.

- Display content of the equipment list

In the equipment list, only FQDN is currently displayed and some people said it is difficult to understand which equipment is supported. Since the number of network devices at home is increasing, it is necessary to establish easy to understand as the standard vendor content for general users (Japanese names, icons, comments assignment by users, etc).

- Access restriction function

The equipment list displays information on all devices in the home and some people said we need to have a user-defined function to control which devices are displayed. If you take privacy and safety of the device into consideration (for example, children cannot operate devices that use fire, etc.), it will be necessary to provide a screen to refer to equipment on an individual or group basis or a function that can set access levels for each equipment (parental lock function, etc.).

In addition, this time, we used a method in which only the translator is registered in the external DNS server and the address of devices in the home are managed by the translator. However, to avoid leaking of device information held in the home, a function to control device access is required.

(2) Security function

- Access from outside the home

One opinion expressed was that the users felt insecure in that there was no phase wherein users were not asked to confirm that they wanted to perform IPsec communication. We need an easy to understand mechanism to make users feel safe, such as providing a confirmation by ID/password beforehand or displaying a mark on the screen that indicates that encrypted IPsec communication is ongoing.

- Security service

User requests with regard to security are sometimes very strong and setting work is naturally troublesome. The results of a survey indicated that more people answered that they would prefer to use a security service than answered that they can configure security-related settings such as a firewall and filtering at home on their own.

With regard to IPv4, many devices (routers, etc.) are provided with typical pre-set patterns. On the other hand, there are no such patterns for IPv6, therefore, there are some cases in which communication may be controlled individually. As IPv6 devices spread, it is necessary to build in such simple setting patterns in devices or provide such services at reasonable cost.

- Power conservation

The primary reason for us to turn off the power of the IP camera this time was to conserve battery life. However, in order to provide steady IPv6-based E2E communication services, the translator and other devices must always be turned ON (during standby as well) and we need to further reduce device power consumption.

(3) Protocol conversion function

- Function implementation device

In our experiment, we used a translator and router as separate devices. An opinion was expressed that since there are many common setting items the two devices could be integrated. If you think about the installation location and troublesome connection, there is no advantage in having separate devices. Therefore, each function needs to be integrated into devices such as routers and servers in future.

- Communication inside and outside the home

In the experiment, protocol conversion was initiated by a DNS request from client devices to the translator. With regard to communication in the home, there is no problem having the translator serve as the DNS server. However, for communication from outside the home, the DNS service is provided by an ISP, therefore, protocol conversion does not take place.

Therefore, when protocol conversion must be performed for communication from outside the home, it is necessary to provide the conversion table with a manual registration function.

6. Guideline for Wireless LAN Access Segment

6.1 Overview

This chapter discusses the IPv6 deployment guideline intended for wireless LAN access delivery service. In Part 2, an actual IPv6 deployment model case environment is built for a wireless LAN access point system installed on the street compliant with the IEEE 802.11a/b/g standard and the specific deployment method for IPv6 in the said environment is introduced in which solutions actually fulfill requirements, and implemented advantages and associated issues are described.

6.2 Typical Deployment Scenario for Wireless LAN Access System

The following method was demonstrated as a typical deployment scenario for the wireless LAN access point system.

Concerning the deployment scenario mentioned in this chapter, the focus is on IPv6 deployment in such a manner as to not impact the existing IPv4 service. If an entire wireless LAN access point system is going to be newly built, issues and problems with the construction of the basic wireless LAN access point system need to be resolved, however, there are no constraints on compatibility with systems used to implement existing services. Therefore, this scenario does not deal with IPv6 deployment scenario in that the network and server equipment are simply installed to be compliant with IPv6, whereas, studies are underway to specialize in a model in which IPv6 deployment focuses on the existing equipment to the maximum while continuously promoting the existing IPv4 service.

Assuming the wireless LAN access point system allows end users to use various Internet services by logging onto a wireless LAN access point, this scenario is studied with the focus placed on the following issues:

- IPv6 deployment does not cause major changes to the series of operations that take place from the IPv4 network connection to the Internet connection.
- Access from the existing IPv4 service to IPv6 service must be possible.
- Even if end users or service providers migrate to IPv6, connectivity to the existing environment can be retained.

6.2.1 Prior to IPv6 Deployment

Figure 6.2.1.1 shows a typical example of an existing wireless LAN access system configuration prior to IPv6 deployment. On the network in this example, ends users connect to an IPv4-compliant wireless LAN access system via an IPv4 terminal, and service providers connect to the same system via an IPv4 server.

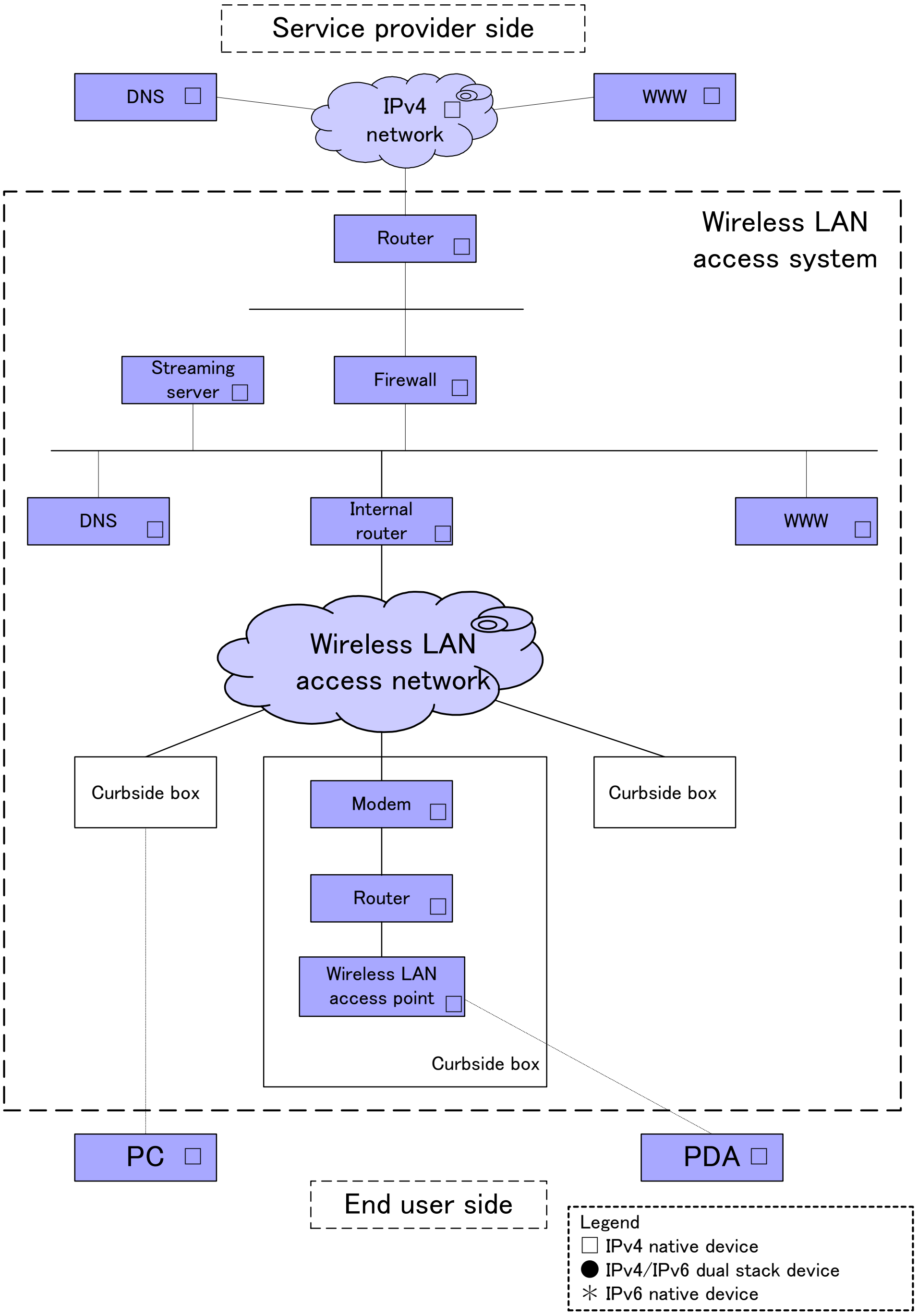


Figure 6.2.1.1: Configuration Prior to IPv6 Deployment

6.2.2 IPv6 Deployment Period

Figure 6.2.2.1 shows the method of IPv6 deployment for this model.

If the destination of wireless LAN access points on the street differs depending on whether IPv4 or IPv6 is used, end users must change the destination with the above circumstances kept in mind, thus making seamless deployment harder than ever. This deployment model allows end users to use IPv6 at the same wireless LAN access point. End users will be able to migrate to IPv6 with their own PC, PDA or terminal simply by making them IPv6-compliant with the same destination.

On the other hand, service providers on the Internet side must have an environment that is capable of providing services for both IPv4 and IPv6 end users. Therefore, the wireless LAN access system will offer connection to the IPv4/IPv6 Internet. Concerning the equipment (router, firewall) connected to the Internet via IPv4 and IPv6, for reasons mentioned below a discrete configuration is used to minimize impact on the existing IPv4 service.

- Firewall

While IPv4 networks have difficulty with delivery of global addresses for all terminals and depend on network address conversion (NAT), IPv6 networks allow all unique global addresses to be delivered, eliminating the need for address conversion. Why? Because the address of end user terminals is masked by NAT equipment and thus direct connectivity from the Internet can be blocked, whereas, IPv6 allows connectivity from the Internet to be provided for all terminals so that the description of security policies for filtering tends to be complex. This is why a discrete configuration is used to eliminate impact on the performance of IPv4 service.

- Router

Because failure in upstream connection routers impacts all existing services, they are separated from IPv4 routers for existing services, which require stable operation.

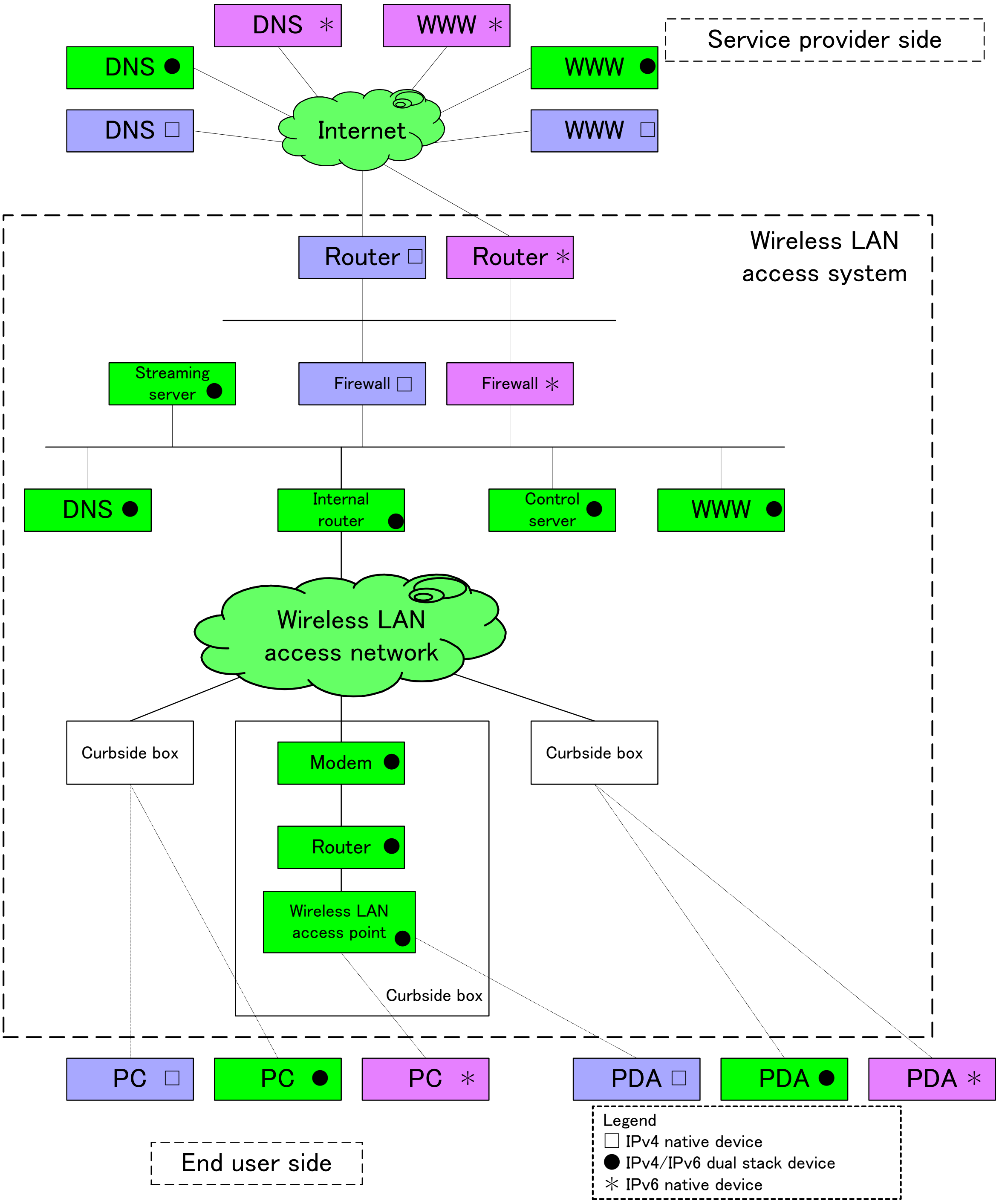


Figure 6.2.2.1: Configuration IPv6 Deployment

6.3 Specific Cases

As specific cases, the following sections relate to circumstances witnessed when the IPv6 deployment model was verified by means of an actual wireless LAN access system.

6.3.1 Model Cases

The wireless LAM access system in Part 2 is outlined here.

The wireless LAN access points are housed together with routers or modems in curbside boxes scattered over a specific geographical area.   An end user connects his or her PC to a wireless LAN access point on the street. The processed content of the curbside box is fed into a data center via ADSL lines.

The data center includes a certificate server responsible for authentication at wireless LAN access points, a router within the curbside box, DNS servers that bind an IP address and name, service-related servers such as Web and streaming servers, and management-related servers such as a monitoring server and administration server.

Upstream connections are connected to the already IPv4/IPv6 dual stack-compliant Internet via a firewall.

Physical Network Configuration

Concerning the configuration referred to in Part 2, Figure 6.3.1.1 shows the physical configuration of the entire network.

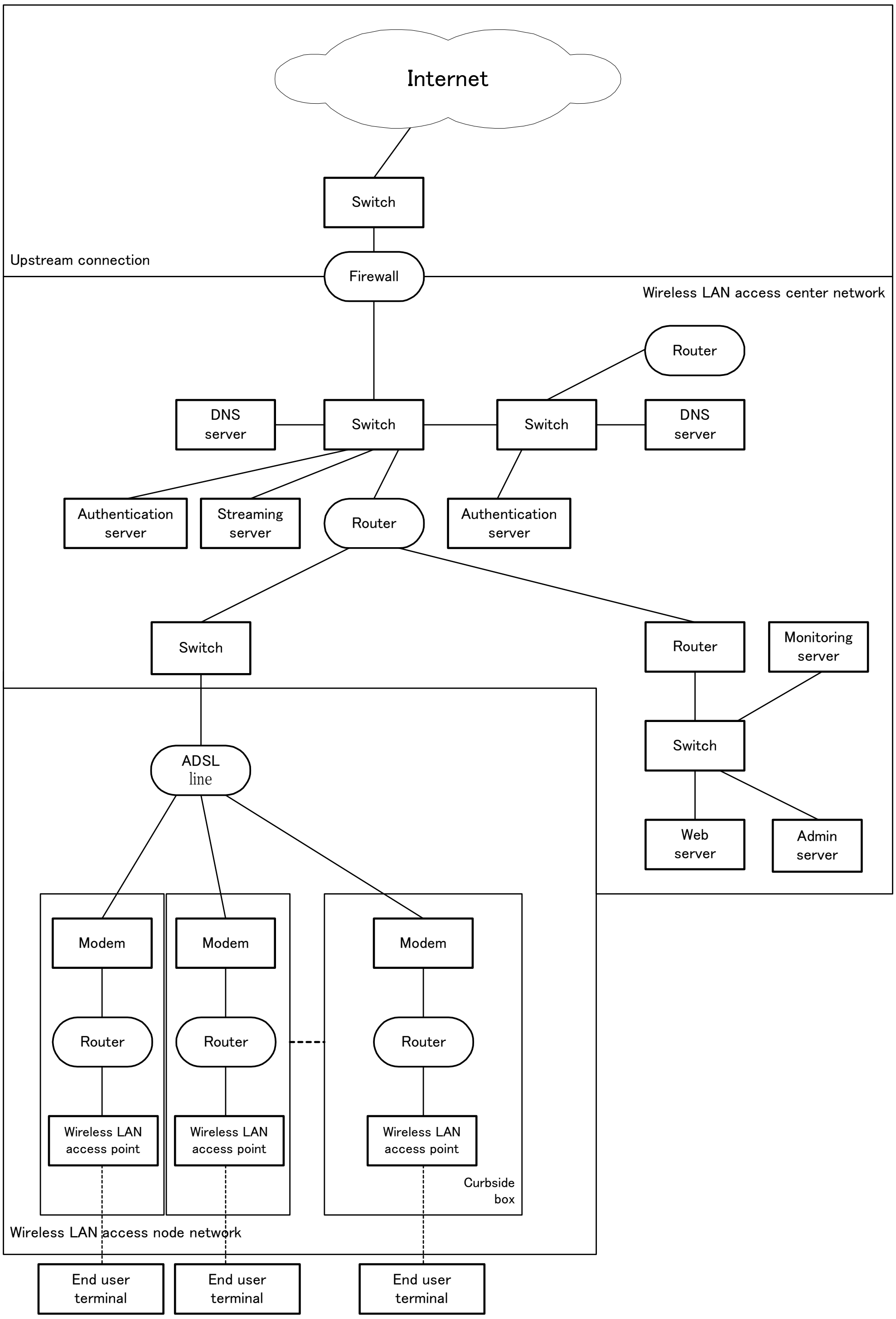


Figure 6.3.1.1: Physical Block Diagram in IPv4 Environment

(1) Upstream connection

Concerning the connection to the Internet at the data center, Ethernet is used for the IPv4 communication line. The communication line is connected to a switch and is expected to be protected from illegal communication by a firewall.

The block diagram for upstream connection is shown in Figure 6.3.1.2 and the associated components are listed in Table 6.3.1-1.

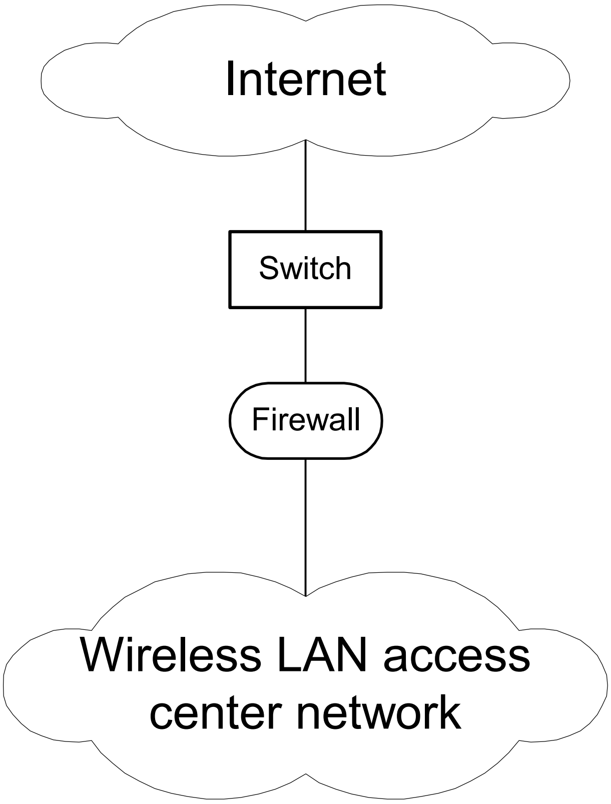


Figure 6.3.1.2: Block Diagram for IPv4 Upstream Connection

Table 6.3.1.1: IPv4 Upstream Connection Equipment List

No.	Host name	Maker	Model	Product name	OS	IPv4 address	Notes
1	aldfw00	Nokia	IP350	NOKIA IP350	FW-1 NG	192.0.2.130/29 192.0.2.144/28	IPv4 firewall
2	aldsw00	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.131/29	Switch

(2) Wireless LAM access center side network

Within the data center, the switches are arranged under the firewall and center servers are connected on the same segment. Moreover, via the internal router, servers are connected to other center servers through Ethernet line connected to another dada center. In addition, communication is connected to wireless LAN access point network installed on the street via ADSL access provider line from the internal router.

A block diagram of the wireless LAN access center network is shown in Figure 6.3.1.3 and the associated components are listed in Table 6.3.1.2.

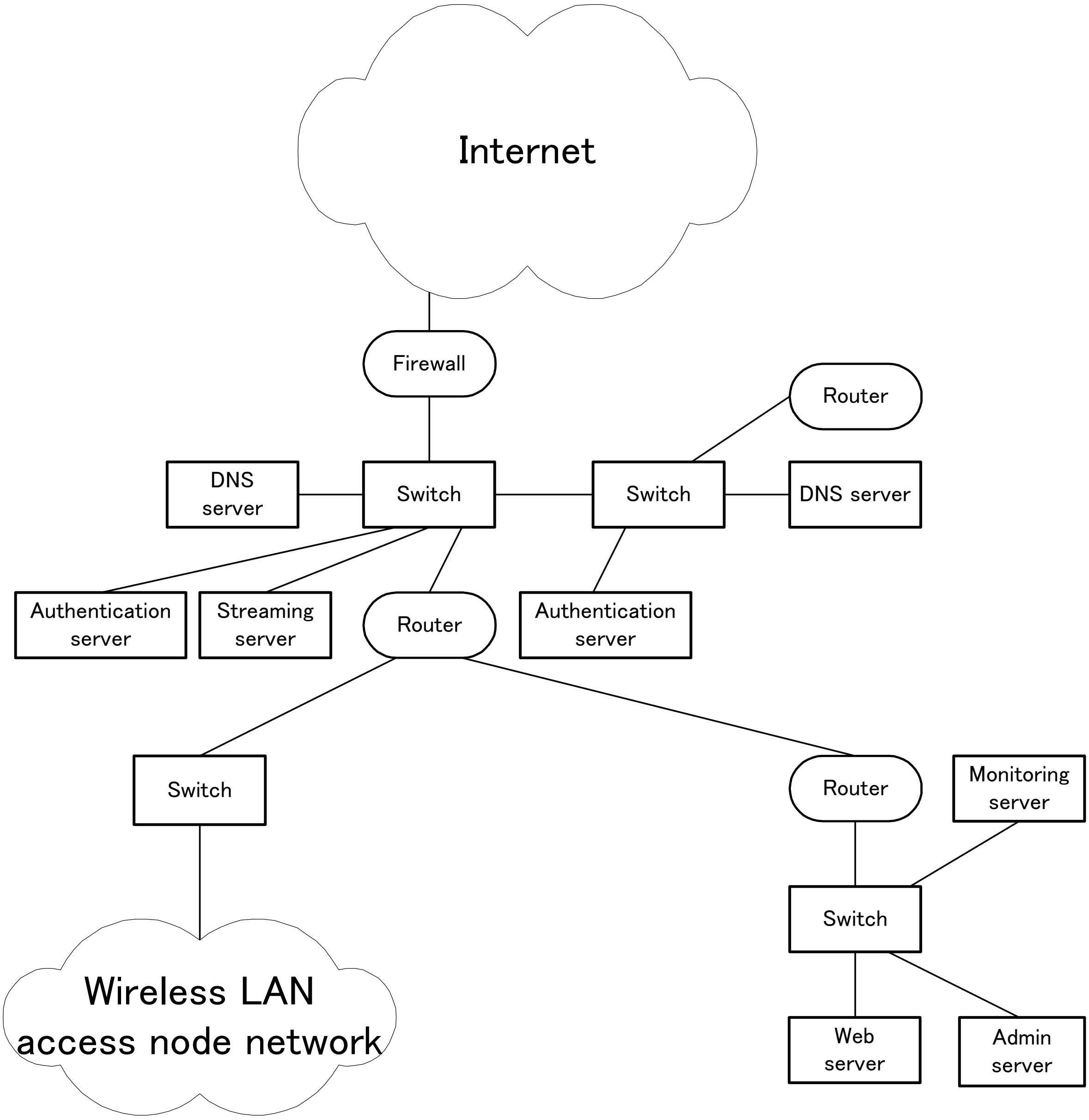


Figure 6.3.1.3: Block Diagram of IPv4 Wireless LAN Access Center Side Network

Table 6.3.1.2: List of Equipment in IPv4 Wireless LAN Access Center Side Network

No.	Host name	Maker	Model	Product name	OS	IPv4 address	Notes
1	aldfw00	Nokia	IP350	NOKIA IP350	Firewall-1 NG	192.0.2.130/29	IPv4 firewall
						192.0.2.144/28	
2	aldrt10	Hitachi	GR2000-2B	Hitachi GR2000-2B	ROUTE-OS6B	192.0.2.151/28	Router
						10.5.51.1/24	
						10.5.52.1/24	
3	aldns00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.147/28	DNS server
4	aldwms00	HP	DL360G3	HP Proliant DL360G3	Windows 2003 Enterprise Edition	192.0.2.150/28	Streaming server

5	aldrd00	HP	DL360G3	HP Proliant DL360G3	Windows2000 Server	192.0.2.149/28	Authentication server
6	aldrd01	HP	DL360G3	HP Proliant DL360G3	Windows2000 Server	192.0.2.152/28	Authentication server
7	aldrp00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.148/28	DNS server
8	aldrt20	IIJ	SEIL/Turbo	IIJ SEIL/Turbo		192.0.2.155/28	Data center installed router
9	aldrt12	HP	DL360G3	HP Proliant DL360G3	Redhat 9	192.0.2.141/29 10.5.51.2/24	Data center installed router
10	aldmon00	HP	DL360G3	HP Proliant DL360G3	Redhat 9	192.0.2.138/29	Monitoring server
11	aldweb00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.139/29	WWW server
12	aldusup0	SUN	V210	SUN V210	Solaris 8	192.0.2.140/29	Management server
13	aldsw00	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.131/29	Switch
14	aldsw10	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.145/28	Switch
15	aldsw11	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.146/28	Switch
16	aldsw20	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	10.5.52.2/24	Switch
17	aldsw30	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.137/29	Switch

(3) Wireless LAN access point network

The network is connected to individual curbside boxes via ADSL access carrier's line. Within the curbside box, access is connected from an ADSL modem to the router providing termination for PPPoE and to wireless LAN access point equipment.

The block diagram of wireless LAN access point network is shown in Figure 6.3.1.4and the associated components are listed in Table 6.3.1.3.

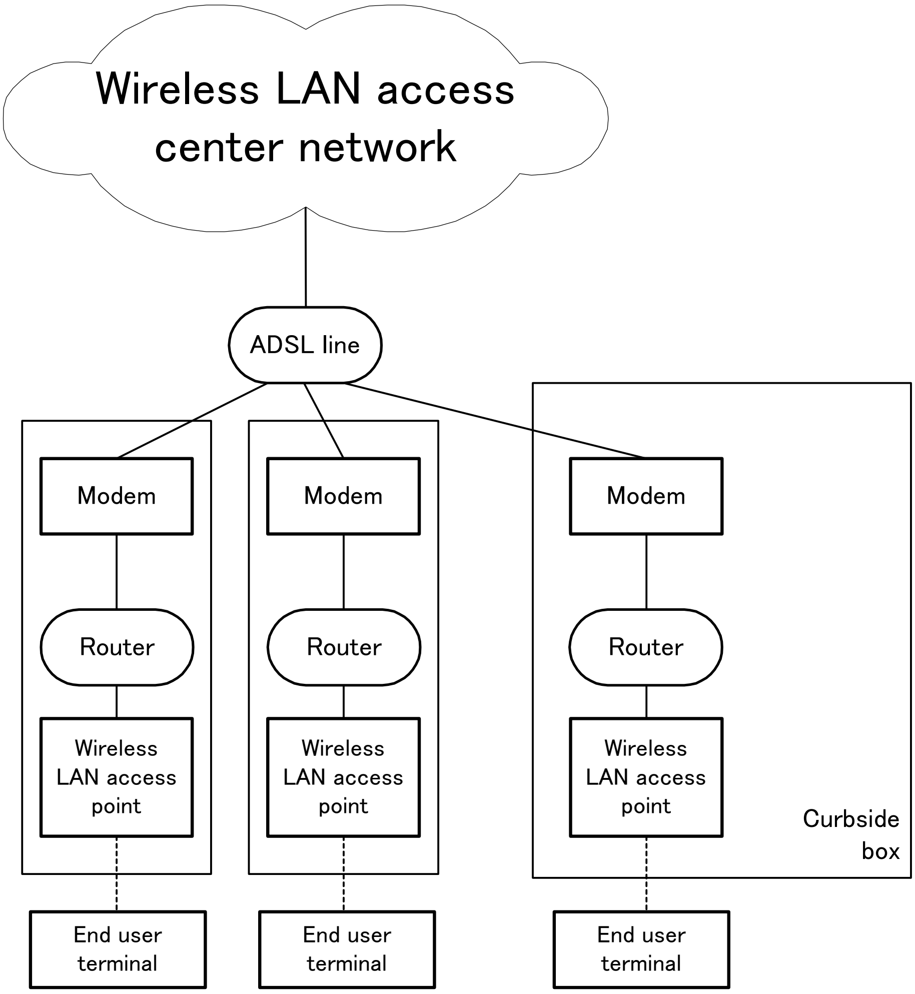

Wireless LAN access center network
ADSL line
Modem
Modem
Modem
Router
Router
Router
Wireless LAN access point
Wireless LAN access point
Wireless LAN access point
Curbside box
End user terminal
End user terminal
End user terminal

Figure 6.3.1.4: Block Diagram of IPv4 Wireless LAN Access Point Network

Table 6.3.1.3: List of Equipment on IPv4 Wireless LAN Access Point Network

NO.	Host name	Maker	Model	Product name	OS	IPv4 address	Notes
1	alvap001	Toshiba	WA-7000	Toshiba WA-7000			Wireless access point
2	alvmd001	Fujitsu	FLASHWAVE 2040	Fujitsu FLASHWAVE2040			Modem
3	alvrt001	IIJ	SEIL/2FE	IIJ SEIL/2FE		10.5.0.128/27 10.5.0.1/27	Wireless access point router

Logical Network Configuration

This section describes the logical configuration of the wireless LAN access system network.

(1) Upstream connection

Concerning upstream connection at the data center, the wireless LAN access system is split into several segments for use with global addresses that it is expected will be allocated. The logical configuration of the upstream connection is shown in Figure 6.3.1.5.

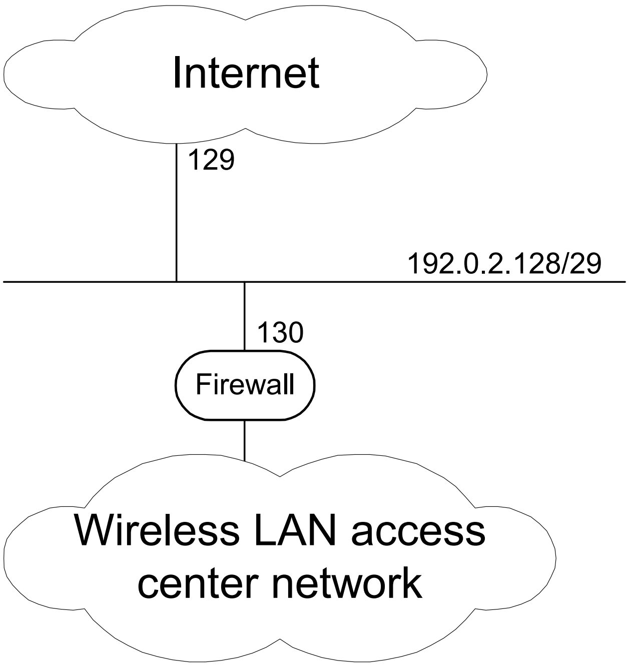


Figure 6.3.1.5: Logical Configuration of IPv4 Upstream Connection

(2) Wireless LAN access center side network

Within the data center, an assortment of servers are connected on the same segment under the firewall. Private addresses are used for the downstream segments of the ADSL access carrier's line.

Logical configuration of the network at the wireless LAN access center side is shown in Figure 6.3.1.6.

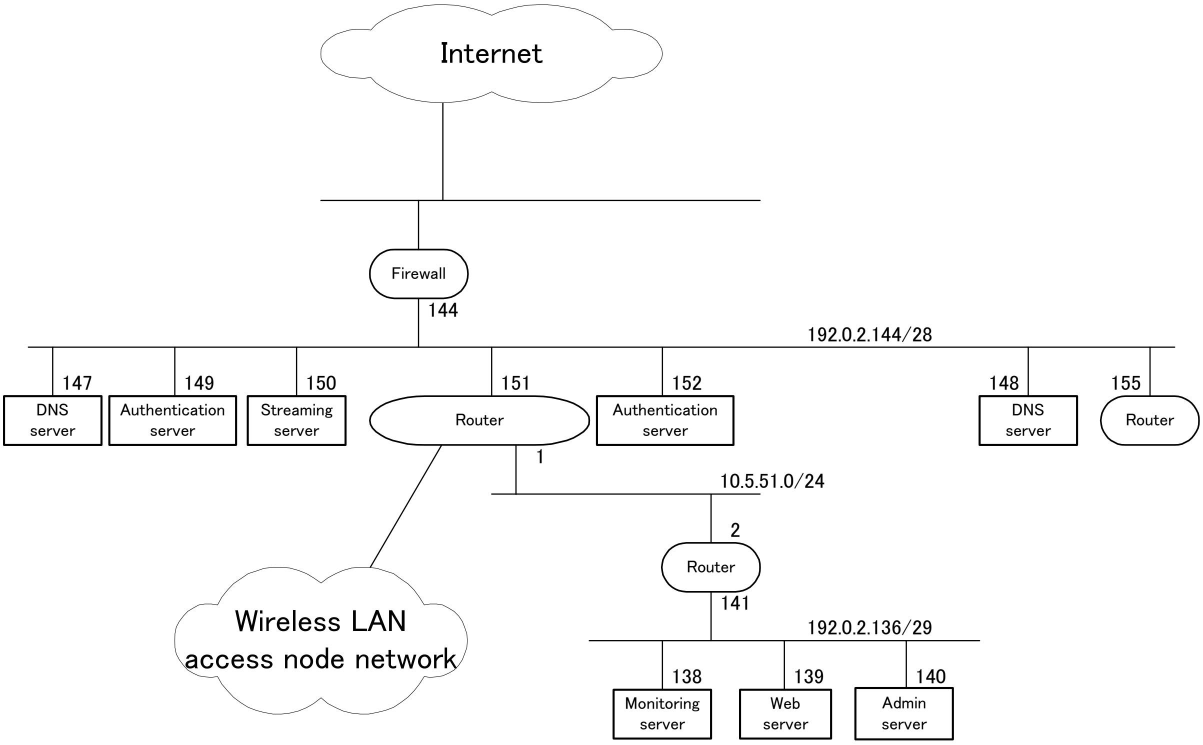


Figure 6.3.1.6: Logical Block Diagram of IPv4 Wireless LAN Access Center Side Network

(3) Wireless LAN access point network

Accesses are connected to each curbside box via an ADSL access carrier line based on a private address. Within the curbside box, lines are configured in separate LANs in the router. The modem is configured with no address assigned.

A logical block diagram of the wireless LAN access point network is shown in Figure 6.3.1.7.

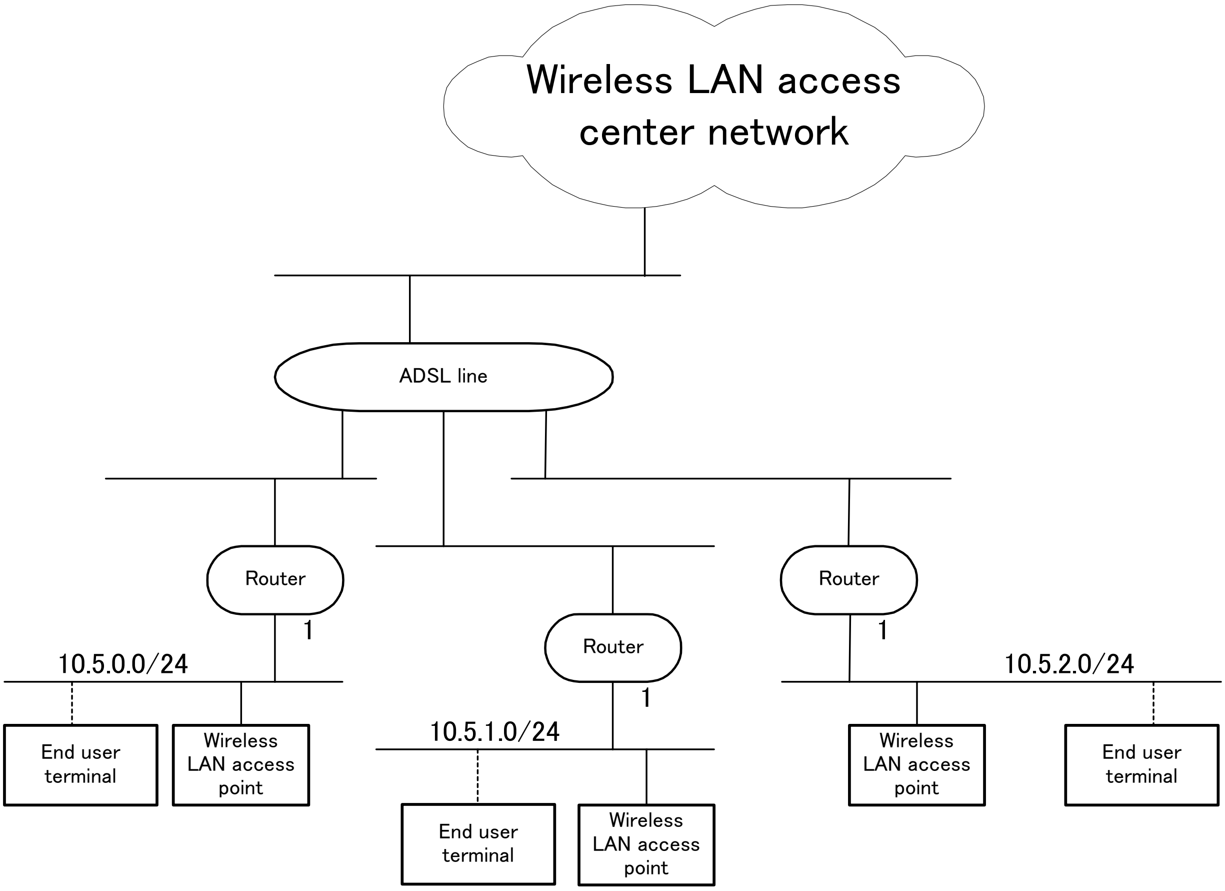


Figure 6.3.1.7: Logical Block Diagram of IPv4 Wireless LAN Access Point Network

Applications

This section describes various services provided by the wireless LAN access system.

(1) Web

The major Web services offered through the wireless LAN access system include delivery of information about the wireless LAN access system intended for end users connected to wireless LAN access points. Table 6.3.1.4 shows details of the configuration of the Web server used.

Table 6.3.1.4: IPv4 Web Configuration Table

No.	Host name	Maker	Model	Product name	OS	IPv4 address	Usage	Application	Notes
1	aldweb00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.139/29	Web server	Apache/2.0.48	

(2) Streaming

A major service provided through streaming applications over the wireless LAN access system is delivery of video by means of streaming for end users connected to wireless LAN access points. Table 6.3.1.5 shows details of the streaming server configuration used.

Table 6.3.1.5: List of IPv4 Streaming Components

No.	Host name	Maker	Model	Product name	OS	IPv4 address	Usage	Applications	Notes
1	aldwms00	HP	DL360G3	HP Proliant DL360G3	Windows 2003 Enterprise Edition	192.0.2.150/28	Streaming server	Windows Media Service 9	

(3) DNS

The main service of DNS via the wireless LAN access system includes delivery of name resolution for end users connected to wireless LAN access points, retention and release of zone information concerning forward and reverse resolution of the wl.v6trans.jp domain, and a v6trans.jp domain slave function. Table 6.3.1.6 shows details of the DNS server configuration used.

Table 6.3.1.6: List of IPv4DNS Components

No.	Host name	Maker	Model	Product name	OS	IPv4 address	Usage	Applications	Notes
1	aldns00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.147/28	DNS server	BIND 9.2.3rc4	Primary
2	aldrp00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.148/28	DNS server	BIND 9.2.3rc4	Secondary

(4) Monitoring

The main monitoring services provided via the wireless LAN access system are checking the operation of network equipment and servers within the wireless LAN access system, and providing a function to alert the administrator in the event of trouble. Table 6.3.1.7 shows details of the monitoring server configuration used.

Table 6.3.1.7: List of IPv4 Monitoring Components

No.	Host name	Maker	Model	Product name	OS	IPv4 address	Usage	Applications	Notes
1	aldmon00	HP	DL360G3	HP Proliant DL360G3	Redhat 9	192.0.2.147/29	Monitoring server		

6.3.2 IPv6 Deployment Cases

This section relates to the wireless LAN access system described in Section 6.3.1 and discusses specific IPv6 deployment methods and the model responsible for IPv6 deployment affecting end users and servers on the Internet side actually connected to the system, as well as the feasibility thereof, and also provides up-to-date information on issues related to IPv6 deployment.

IPv6 Deployment Policy

This section discusses deployment policies related to IPv6 deployment for the said wireless LAN access system.

(1) Overall policy for deployment IPv6

While all equipment under the said wireless LAN access system is basically compliant with IPv6, the policies in the following configuration are applied assuming some constraints on the delivery of service.

Based on these policies, the configurations in the tables allow the existing wireless LAN access systems to be IPv6-compliant.

(a) Minimize effects on existing IPv4 network

Because IP communication provisioning is the most important service in the wireless LAN access system, it is necessary to avoid the creation of an IPv6 deployment environment that causes the existing IPv4 communication to be unstable.

Because of this, a desirable configuration is such that adverse effects should be suppressed to a minimum in areas in which IPv4 and IPv6 might interfere with each other.

(b) Minimize effects on existing IPv4 server services

The same applies to the server service.

(c) Maintain extensive coverage

It is preferable to be compliant with various IPv6 services to the maximum possible extent. It is also desirable for all configurations of the network to be IPv6-compliant.

(d) Deployment cost should be curbed to a minimum

Renewal of equipment is preferably curbed with a view to financial constraints. Based on the above consideration, cost redundancy of the IPv6 network should be to the extent such redundancy is economically feasible.

(e) Management cost should be curbed

A desirable configuration is such that IPv6 network configuration and IPv6 server service configuration should be self-explanatory and easy to manage while placing only the minimum amount of burden on administrators.

(2) IPv6 deployment model applicable to wireless LAN access system

This section describes specific IPv6 deployment methods applicable to equipment connected to a wireless LAN access system compliant with IPv6 in line with the above-mentioned policies.

(a) About the entire network

While the described model is configured with dual stack equipment that provides IPv6 support, certain areas of the configuration are likely to significantly impact IPv4 service, so IPv4-specific equipment and IPv6-specific equipment are separately routed.

(b) Upstream connection

Concerning the above deployment model, as described in Section 6.2.2, the equipment connected to the Internet under IPv4 and IPv6 has many different factors that run counter to each other in terms of functionality, so they are separately configured to suppress impact on existing IPv4 services as much as possible.

(c) Wireless LAN access center side network

Because the network equipment in the wireless LAN access center uses a dual stack configuration, IPv6 address processing was initiated on the same equipment. Because the servers connected on the wireless LAN access center side ran on operating systems that provide dual stack support, IPv6 processing was initiated to implement delivery of IPv6 service.

(d) Wireless LAN access point side network

As the form of connection from end users, the configuration is not designed to change the destination of access for IPv4 and IPv6, whereas, alternative configurations allow the destination of access to remain unchanged and to be accessible to both networks depending on the type of terminal in use. Because of this, service is provided in a dual stack environment using the same equipment to allocate IPv6 addresses.

(e) IPv6-compliant equipment connected to wireless LAN access points

As mentioned above, the wireless LAN access system is supposed to be compliant with IPv4/IPv6. A translator that provides IPv4-IPv6 conversion and vice-versa is installed to provide usual connectivity to IPv4 networks for connection from existing IPv4 terminals, and to enable IPv6 communication via the translator. As soon as end users become ready, upgrade to IPv4/IPv6 dual stack equipment or IPv6 native equipment will be performed to implement IPv6 deployment. Even when IPv6 deployment is in place, service can be delivered via the translator, so that upgrades will not make existing services unavailable.

(f) IPv6 deployment on the service provider side

The wireless LAN access system is prepared in an dual stack IPv4/IPv6 environment, and moreover, a translator provides IPv4-IPv6 conversion and vice-versa. Therefore, the existing IPv4 service provider continues to provide IPv4 communication as usual for connections from end users, and service is provided to IPv6 terminals as well via the translator. After IPv6 deployment is in place, service can be delivered to existing IPv4 terminals via the translator. This allows for configuration designed to eliminate or minimize the chance of loss of end user connectivity and service provisioning.

Physical Network Configuration

Figure 6.3.2.1 shows the overall physical configuration of the wireless LAN access system.

As mentioned in the policy on IPv6 deployment, because the configuration is designed to suppress the impact on IPv4 service, upstream communication lines and firewalls are separately arranged to deal with the possibility of drastic changes in usage patterns, such as changes to addresses and filtering policies; unlike IPv4, IPv6 usage patterns may change in conjunction with the extension of upstream equipment.

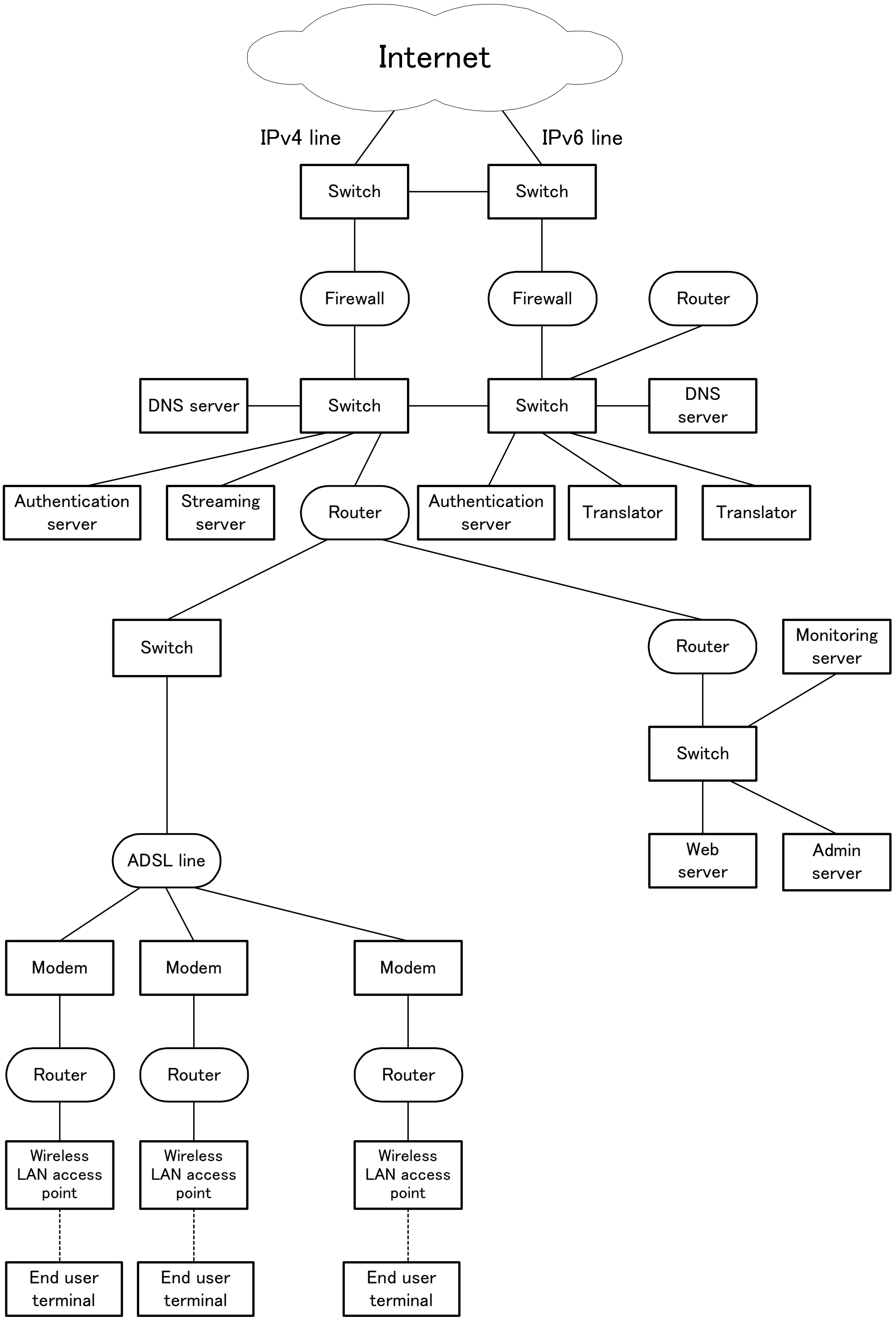


Figure 6.3.2.1: Network Block Diagram upon Deployment

(1) Upstream connection

The data center provides Ethernet-based individual communication lines in IPv4 and IPv6 separately for the connection from the IIJ backbone to the Internet. The lines are connected to the switches and separately connected to IPv4 and IPv6 firewalls.

Figure 6.3.2.2 shows a block diagram of upstream connection and Table 6.3.2.1 shows the associated components.

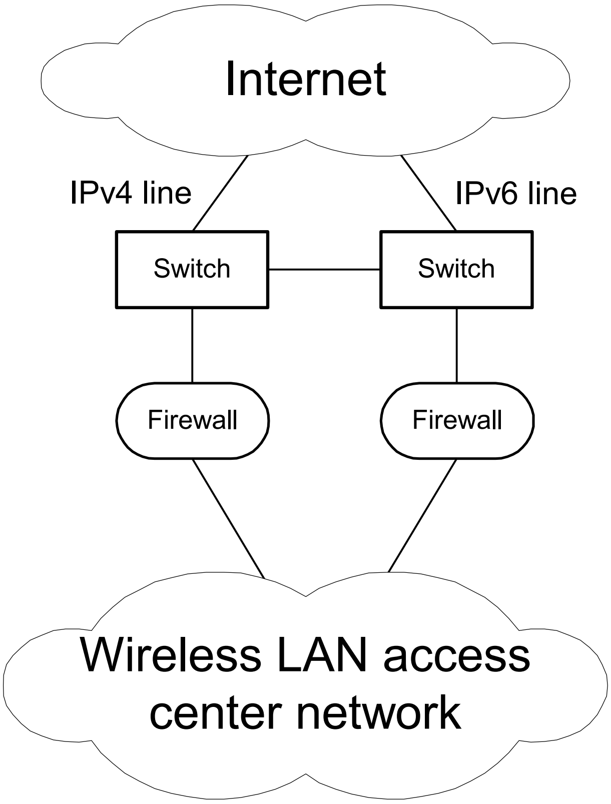


Figure 6.3.2.2: Block Diagram of Upstream Connection upon Deployment

Table 6.3.2.1: List of Upstream Connection Equipment upon Deployment

No.	Host name	Maker	Model	Product name	OS	IPv4 address	IPv6 address	Notes
1	aldfw00	Nokia	IP350	NOKIA IP350	Firewall-1 NG	192.0.2.130/29 192.0.2.144/28		IPv4 firewall
2	aldfw01	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9		2001:db8:5000:ff00::6/64 2001:db8:5000:f400::3/64	IPv6 firewall
3	aldsw00	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.131/29		Switch
4	aldsw01	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.132/29		Switch

(2) Wireless LAN access center side network

Within the data center, switches are arranged downstream from firewalls and an assortment of center servers are connected on the same segment. They are also connected to other center servers via Ethernet and to other data centers via an internal router. In addition, connection is also routed from the internal router to the

ADSL carrier lines.

Figure 6.3.2.3 shows a block diagram of a wireless LAN access center network and Table 6.3.2.2 lists the associated components.

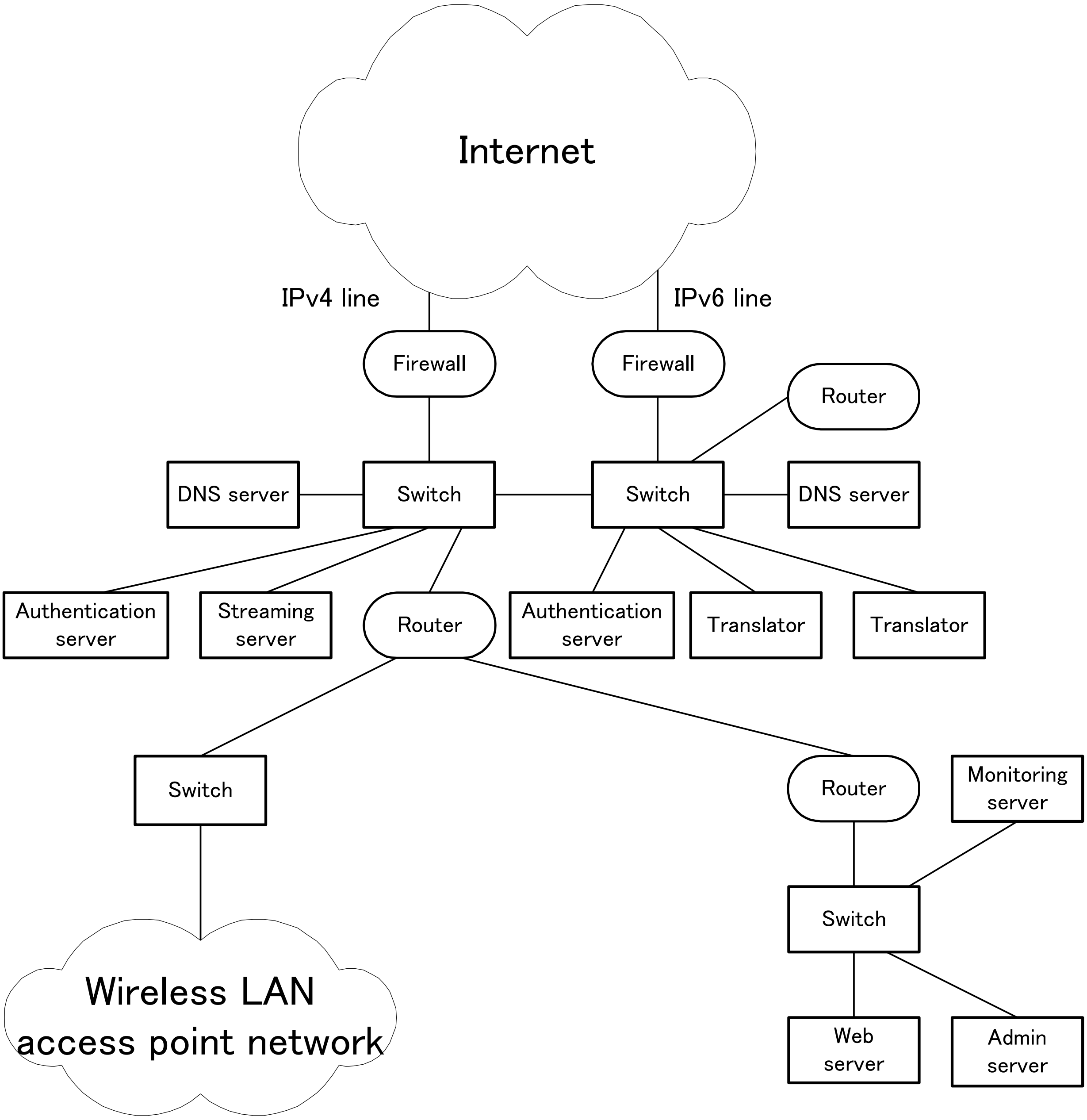


Figure 6.3.2.3: Block Diagram of Wireless LAN Access Center Network upon Deployment

Table 6.3.2.2: List of Wireless LAN Access Center Network Equipment upon Deployment

No.	Host name	Maker	Model	Product name	OS	IPv4 address	IPv6 address	Notes
1	aldfw00	Nokia	IP350	NOKIA IP350	Firewall-1 NG	192.0.2.130/29		IPv4 firewall
						192.0.2.144/28		
2	aldfw01	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9		2001:db8:5000:ff00::6/64	IPv6 firewall
							2001:db8:5000:f400::3/64	
3	aldrt10	Hitachi	GR2000-2B	Hitachi GR2000-2B	ROUTE-OS6B	192.0.2.151/28	2001:db8:5000:f000::2/64	Router
						10.5.51.1/24	2001:db8:5000:f400::4/64	
						10.5.52.1/24	2001:db8:5000:f200::1/64	
4	aldns00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.147/28	2001:db8:5000:f400::8/64	DNS server
5	aldwms00	HP	DL360G3	HP Proliant DL360G3	Windows 2003 Enterprise Edition	192.0.2.150/28	2001:db8:5000:f400::30/64	Streaming server
6	aldrd00	HP	DL360G3	HP Proliant DL360G3	Windows 2000 Server	192.0.2.149/28	2001:db8:5000:f400::10/64	Authentication server
7	aldrd01	HP	DL360G3	HP Proliant DL360G3	Windows 2000 Server	192.0.2.152/28	2001:db8:5000:f400::12/64	Authentication server
8	aldisips	HP	DL380G3	HP Proliant DL380G3	Redhat 9	192.0.2.153/28	2001:db8:5000:f400::14/64	Translator
9	aldisipm	HP	DL380G3	HP Proliant DL380G3	Redhat 9	192.0.2.154/28	2001:db8:5000:f400::16/64	Translator
10	aldrp00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.148/28	2001:db8:5000:f400::20/64	DNS server
11	aldrt20	IIJ	SEIL/Turbo	IIJ SEIL/Turbo		192.0.2.155/28	2001:db8:5000:f400::22/64	Data center installed router
12	aldrt12	HP	DL360G3	HP Proliant DL360G3	Redhat 9	192.0.2.141/29	2001:db8:5000:f100::4/64	Data center installed router
						10.5.51.2/24	2001:db8:5000:f200::4/64	
13	aldmon00	HP	DL360G3	HP Proliant DL360G3	Redhat 9	192.0.2.138/29	2001:db8:5000:f100::1/64	Monitoring server
14	aldweb00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.139/29	2001:db8:5000:f100::2/64	Web server
15	aldusup0	SUN	V210	SUN V210	Solaris 8	192.0.2.140/29	2001:db8:5000:f100::3/64	Management server
16	aldsw10	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.145/28		Switch
17	aldsw11	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.146/28		Switch
18	aldsw20	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	10.5.52.2/24		Switch
19	aldsw30	Cisco	Catalyst 3750G-24T	Cisco Catalyst 3750G-24T	IOS12.2(18)SE	192.0.2.137/29		Switch

(3) Wireless LAN access point network

Calls are connected via the ADSL access carrier lines to each curbside box. Within the curbside box, calls are connected from an ADSL modem to a router that serves as the PPPoE termination point and again connected to wireless LAN access point equipment.

Figure 6.3.2.4 shows a block diagram of wireless LAN access point network and Table 6.3.2.3 lists the associated components.

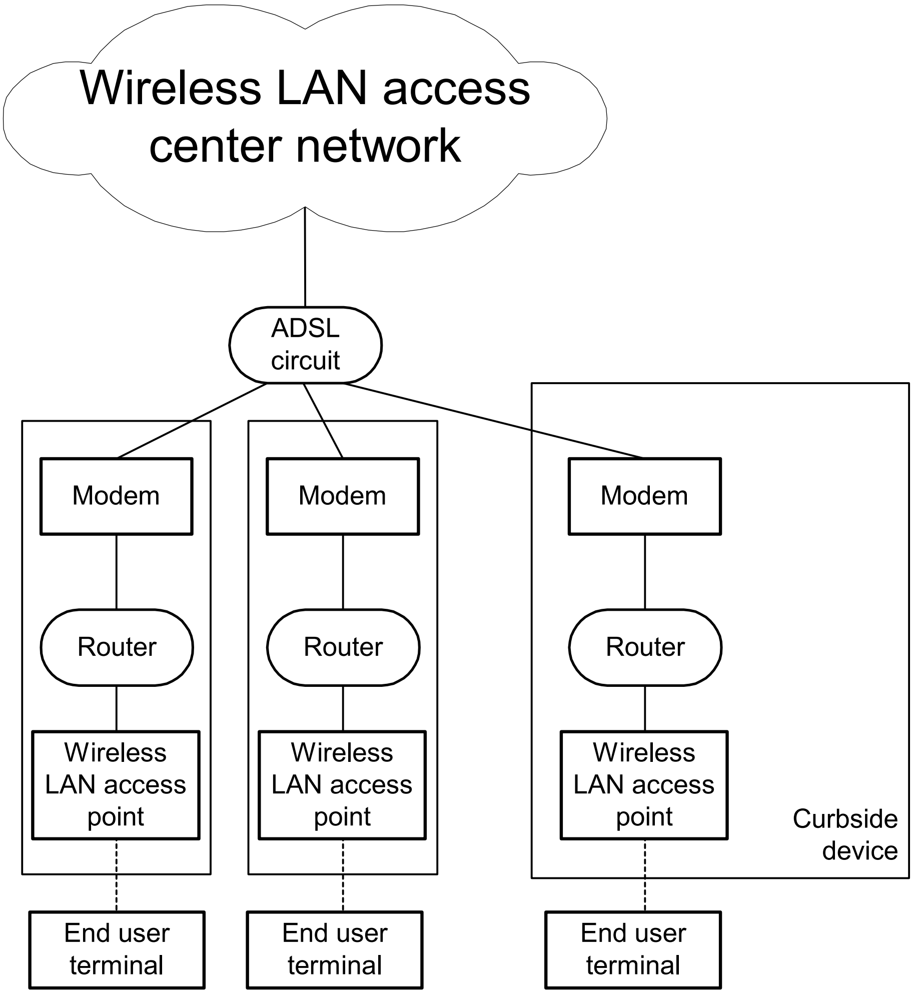


Figure 6.3.2.4: Block Diagram of Wireless LAN Access Point Network upon Deployment

Table 6.3.2.3: Block Diagram of Wireless LAN Access Point Network Equipment upon Deployment

Item no.	Host name	Maker	Model	Product name	OS	IPv4 address	IPv6 address	Remarks
1	alvap001	Toshiba	WA-7000	Toshiba WA-7000				Wireless access points
2	alvmd001	Fujitsu	FLASHWAVE2040	Fujitsu FLASHWAVE2040				Modem
3	alvrt001	IIJ	SEIL/2FE	IIJ SEIL/2FE		10.5.0.128/27	2001:db8:5000:4000::1/64	Wireless access point router
						10.5.0.1/27	2001:db8:5000:0::1/64	

Logical Network Configuration

This section describes the logical network configuration of the wireless LAN access system. The logical configuration of IPv4 and IPv6 segments are described separately.

(1) IPv4 configuration of upstream

The upstream of the data center, as a wireless LAN access system, is divided into separate segments each being assigned a global address.

Figure 6.3.2.5 shows the logical configuration of the upstream.

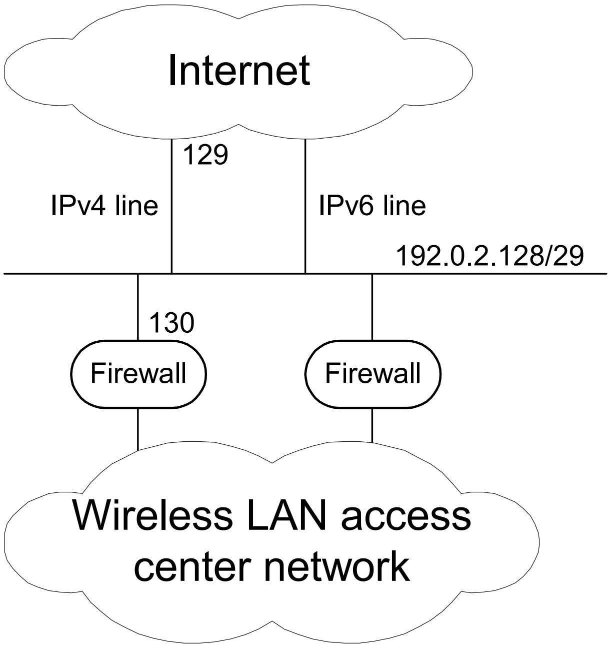


Figure 6.3.2.5: Logical Configuration of Upstream upon Deployment n (IPv4)

(2) IPv4 configuration of wireless LAN access center side network

The center severs in the same segment of the data center inside the firewalls are connected. The servers are connected to segments in other data centers via internal routers. Private addresses are used from ADSL access provider lines.

Figure 6.3.2.6 shows the logical configuration of the network on the wireless LAN access center side.

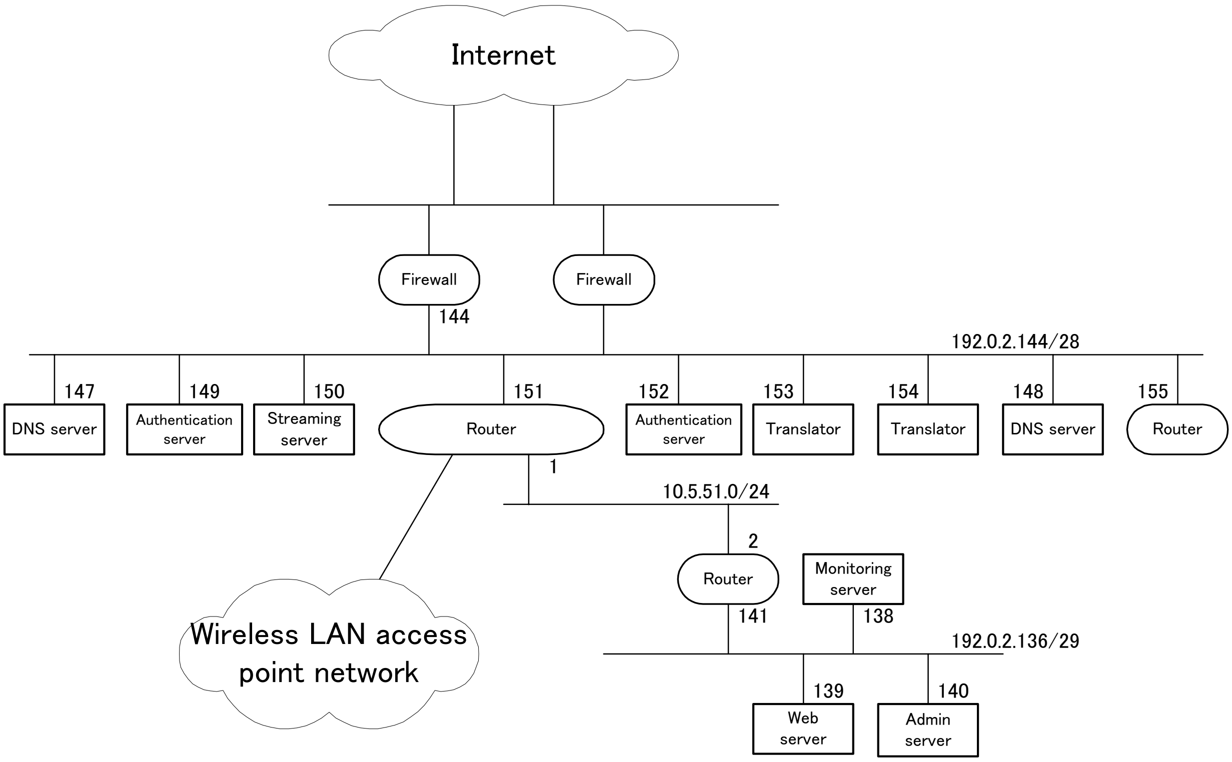


Figure 6.3.2.6: Logical Network Configuration of Wireless LAN Access Center upon Deployment (IPv4)

(3) IPv4 configuration of wireless LAN access point network

Private addresses are used to connect the network to access points via the ADSL access provider lines. Each access point is equipped with a router that connects two VLANs. However, addresses are not used with modems.

Figure 6.3.2.7 shows the logical configuration of the wireless LAN access point network.

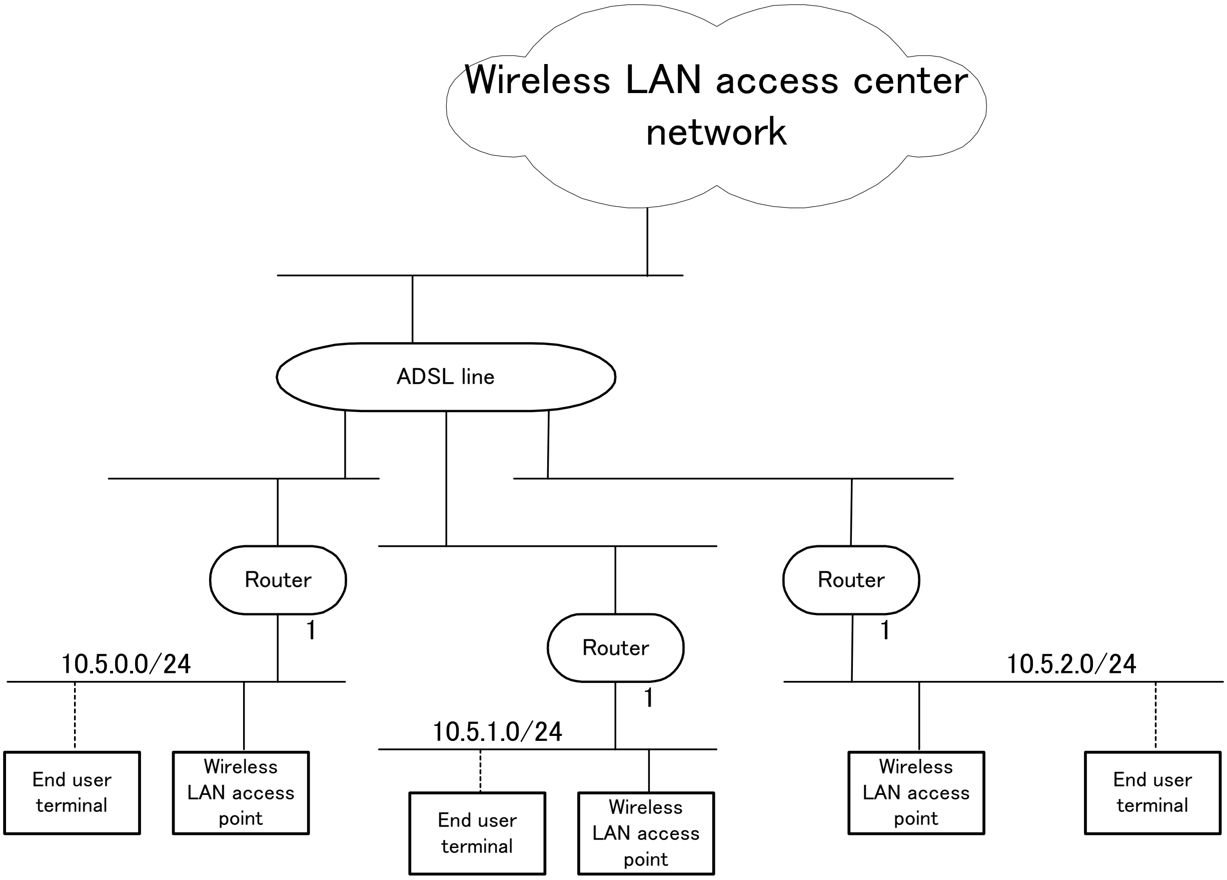


Figure 6.3.2.7: Logical Configuration of Wireless LAN Access Point Network upon Deployment (IPv4)

(4) Configuration of IPv6 upstream

The upstream of the data center in the wireless LAN access system consists of multiple segments each of which are assigned an IPv6 address.

Figure 6.3.2.8 shows the logical configuration of the upstream.

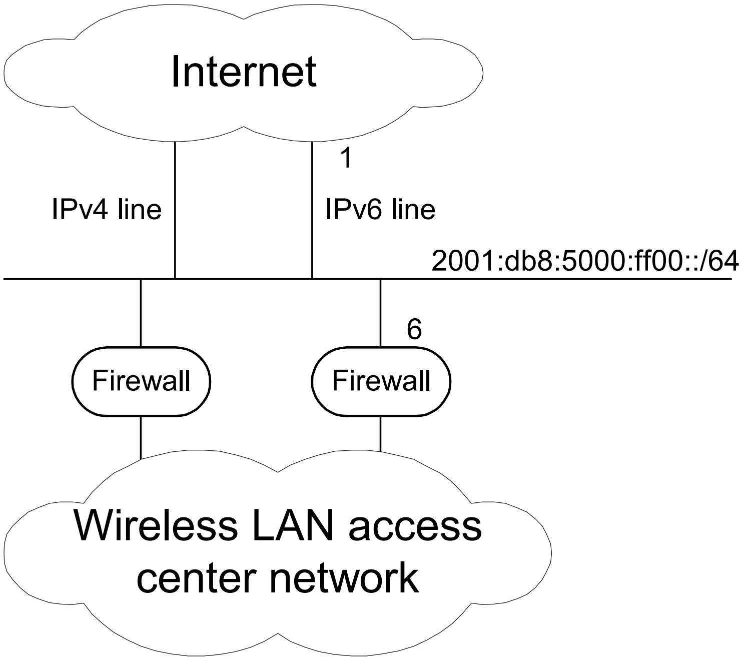


Figure 6.3.2.8: Logical Configuration of Upstream upon Deployment (IPv6)

(5) IPv6 configuration of wireless LAN access center network

The center servers in the same data center segments inside the firewall are connected. Internal routers ADSL access provider lines are also connected.

Figure 6.3.2.9 shows the logical configuration of the wireless LAN access center network.

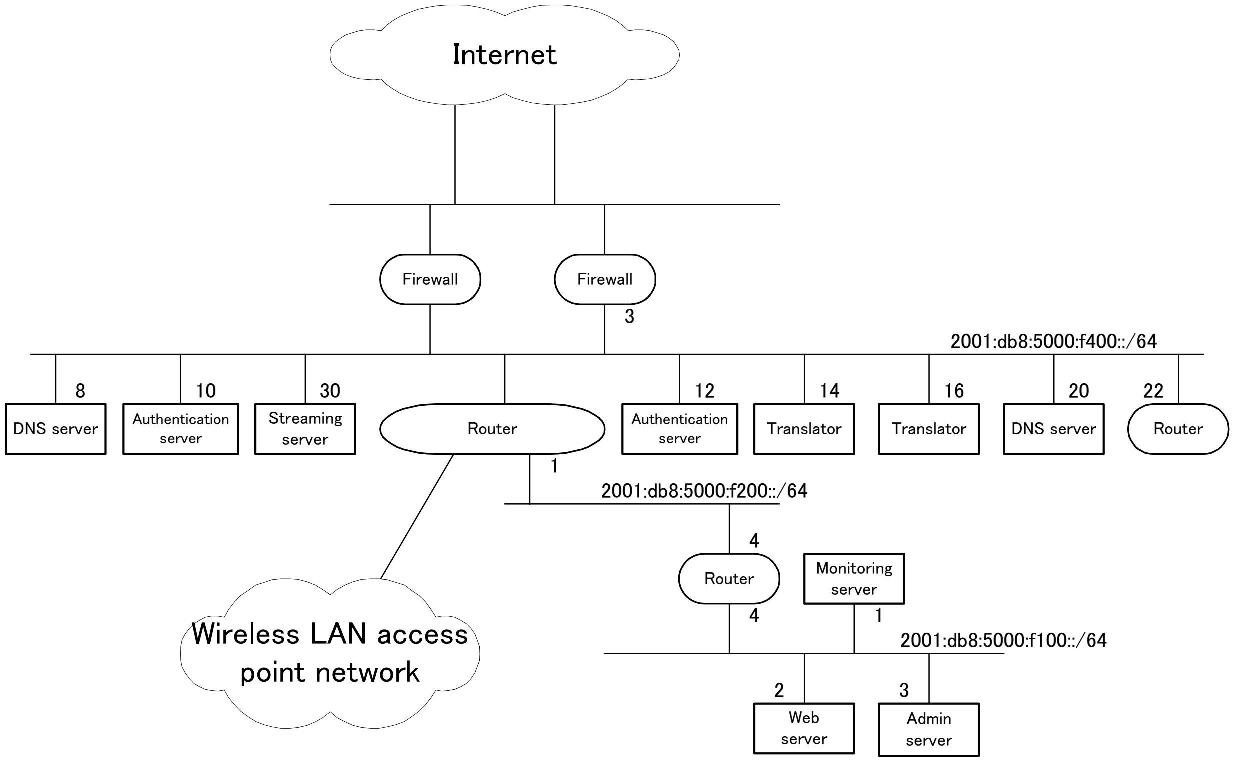


Figure 6.3.2.9: Logical Configuration of Wireless LAN Access Center Network upon Deployment (IPv6)

(6) IPv6 configuration in wireless LAN access point network

The network is connected to an access point via an ADSL access provider line. Each access point is equipped with a router that connects two VLANs. However, addresses are not used with modems.

Figure 6.3.2.10 shows the logical configuration of the wireless LAN access point network.

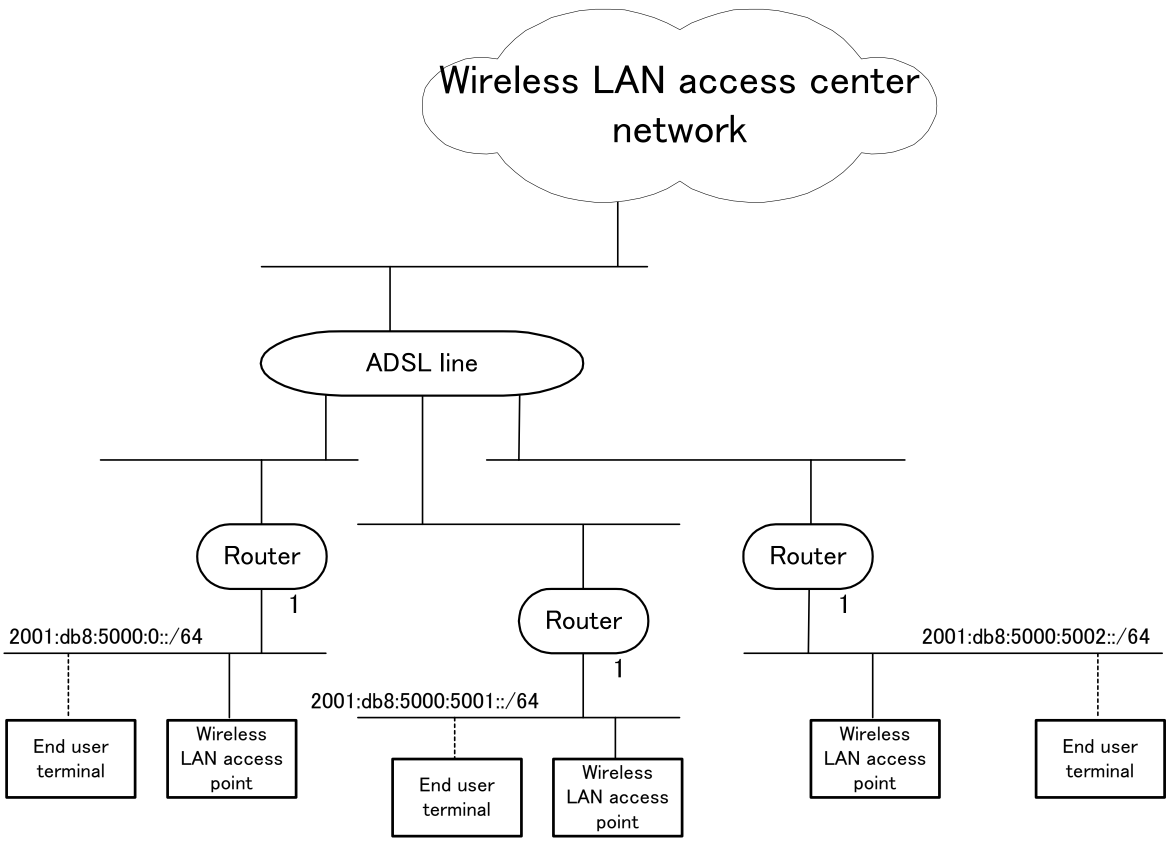


Figure 6.3.2.10: Logical Configuration of Wireless LAN Access Point Network upon Deployment (IPv6)

Applications

The following sections describe services provided by the wireless LAN access system.

(1) Web

The major Web services offered through the wireless LAN access system include delivery of information about the wireless LAN access system intended for end users connected to wireless LAN access points. Table 6.3.2.4 shows details of the configuration of the Web server used.

Table 6.3.2.4: Web Configuration upon Deployment

No.	Host	Maker	Model	Product	OS	IPv4 address	IPv6 address	Usage	Application
1	aldweb00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.139/29	2001:db8:5000:f100::2/64	Web server	Apache/2.0.48

(2) Streaming

A major service provided through streaming applications over the wireless LAN access system is delivery of video by means of streaming for end users connected to wireless LAN access points. Table 6.3.2.5 shows details of the streaming server configuration used.

Table 6.3.2.5: Streaming Configuration upon Deployment

No.	Host	Maker	Model	Product	OS	IPv4 address	IPv6 address	Usage	Application
1	aldwms00	HP	DL360G3	HP Proliant DL360G3	Windows 2003 Enterprise Edition	192.0.2.150/28	2001:db8:5000:f400::30/64	Streaming server	Windows Media Service 9

(3) DNS

The main service of DNS via the wireless LAN access system includes delivery of name resolution for end users connected to wireless LAN access points, retention and release of zone information concerning forward and reverse resolution of the wl.v6trans.jp domain, and a v6trans.jp domain slave function. Table 6.3.2.6 shows details of the DNS server configuration used.

Table 6.3.2.6: DNS Configuration upon Deployment

No.	Host	Maker	Model	Product	OS	IPv4 address	IPv6 address	Usage	Application
1	aldns00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.147/28	2001:db8:5000:f400::8/64	DNS server	BIND 9.2.3rc4 (primary)
2	aldrp00	HP	DL360G3	HP Proliant DL360G3	FreeBSD 4.9	192.0.2.148/28	2001:db8:5000:f400::20/64	DNS server	BIND 9.2.3rc4 （secondary）

(4) Monitoring

The main monitoring services provided via the wireless LAN access system are checking the operation of network equipment and servers within the wireless LAN access system, and providing a function to alert the administrator in the event of trouble. Table 6.3.2.7 shows details of the monitoring server configuration used.

Table 6.3.2.7: Configuration of Monitoring upon Deployment

No.	Host	Maker	Model	Product	OS	IPv4 address	IPv6 address	Usage	Application
1	aldmon00	HP	DL360G3	HP Proliant DL360G3	Redhat 9	192.0.2.138/29	2001:db8:5000:f100::1/64	Surveillance server	

6.3.3 Evaluation

The following is an evaluation of the results of the IPv6 deployment model in the wireless LAN access network.

This assessment checks the connectivity and compatibility of equipment connected to the wireless LAN access points and service provider equipment. Finally, a Tips section has been added to provide information on the deployment model that has become available during verification.

Evaluation Items

(1) Routing verification

The verification checked whether the environment permitted regular user terminals such as an IPv4 native client, IPv6 native client or IPv4/IPv6 dual client to connect to the Internet.

IPv6 uses RouterAdvertise (RA) to automatically assign addresses to clients. RA uses the prefix assigned to a router to access the MAC address for the network interface of each client terminal to automatically and accurately issue addresses in IPv6.

However, the equipment used this time was designed to prevent connection to a wireless LAN access point from an unknown MAC address, which made initial handover via RA impossible in IPv6. The reason is that an RA starts transmission to multiple nodes using a MAC address that is not its own and this causes the wireless access point to drop the packet since it cannot identify the MAC address. This made clear that wireless LAN access points need to be able to cope with IPv6 communications.

ADSL lines were used for wireless access point nodes (node boxes) to provide clients with access. PPPoE authentication is sent to the ADSL access provider line and the authentication server (Radius) located in the center performed the registered authentication. Then the setting of attributes by Radius in the router for automatically assigning IPv6 addresses operated normally. Since the Radius server used in this verification did not register attributes for IPv6 by default, a new setting had to be made. It was also established that RIP, RIPng, OSPFv2, OSPv3 and BGP+ operates as intended in other systems.

(2) Verification of system management

Centralized management will be introduced to handle the vast number of network devices that are expected to be connected with the implementation of IPv6. A graphical user interface (GUI) will simplify the addition of devices to the network and enable the following centralized management functions.

- Registration of new devices

This function will make it possible to use the GUI for setting up network connections. All that will be required is to insert a network cable in a router, turning on the power, and automatically download the configuration from the center server via HTTP communication and complete the setup of network connection.

- Changing settings

This function will make it possible to change the router setting in the GUI and transfer this setting automatically from center server to router in the node.

- Returning settings

This function will make it possible use the GUI to return settings to the state they had before a change when the new settings cause malfunctions. This change is transferred from the center server to the node router where the actual change is made.

- Equipment replacement

After replacing a failing device with a new device, this function makes it possible to automatically reflect the settings to the new device and connect it to the network by entering their serial numbers in the GUI.

- Batch registration

When multiple new devices are to be installed simultaneously, this function reflects the settings in GUI, and as soon as the network cables are connected to the devices and the power is turned on, the settings are downloaded from the center server to complete network connection.

It was also possible to perform device monitoring of IPv6 native devices and IPv4/IPv6 dual stack devices in the same way as IPv4 native devices.

(3) Verification of applications

The operating systems of web servers and streaming servers as well as applications have become more IPv6 compliant. It has been established that wireless LAN access systems can easily cope with IPv4 native, IPv6 native and IPv4/IPv6 dual stack environments. This indicates that wireless LAN access systems are now ready for a gradual migration to IPv6.

This experiment will involve the verification of Apache and WindowsMediaServer, two widely used applications. In addition to these, there are a large number of both commercial and non-commercial applications whose conformance to IPv6 will have to be tested. The wireless LAN access system conforms to a dual environment so if individual applications also become compliant, it will be possible to gradually migrate to an IPv6 service.

(4) Network security verification

IEEE802.1x compliant encrypted communications have been tested in wireless LAN access points in this model and it has have proved to enable normal operation from authentication to connection. The following functions, which have been verified to check the security of wireless LANs, work normally in IPv4 native, IPv6 native and IPv4/IPv6 dual environments

- SSID (Service Set Identifier)

The ID of a destination access point and only a wireless LAN terminal with the same SSID can connect to it.

- IEEE802.1x authentication

The Radius server at the center and the access control (authentication) of users that access the network ensures a high degree of security. The system also uses PEAP (Protected Extensible Authentication Protocol), authentication through certification, for even greater security.

- VLAN authentication

Only authenticated users can access a server or network from a wireless LAN access point. This function provides a connection to VLAN and permits only a restricted number of authenticated users, specific servers and specific networks access to the wireless LAN access point.

(5) Multicast verification

This verification of multicasting was made by sending data using PIM-SM to terminals connected to a wireless LAN access point. An IPv6-IPv6 tunnel was used between the center and the node to transfer PIM-SM. This was because the BAS of the ADSL service provider line did not comply with PIM-SM preventing transfer to the node via the normal route. However, the upper limit set for tunnels meant that the environment had to be enhanced by adopting a native multicast routing protocol. As soon as a BAS compliant system is in place, native multicast delivery should be verified.

(6) Verification of gateways

Proxy type translation should be adopted for a wireless LAN access system to enable regular users to use both IPv4 and IPv6 services after migration. It was established that service providers are able to provide services for both IPv4 and IPv6 clients. An issue was what connections a dual stack server should give priority to in the following translation service situations.

- When a connection is made from an IPv4 terminal, the server
  - ➢ connects using IPv4
  - ➢ connects converting to IPv6
- When a connection is made from an IPv6 terminal, the server
  - ➢ connects using IPv6
  - ➢ connects converting to IPv4
- When a connection is made from a IPv4/IPv6 dual stack terminal, the server
  - ➢ connects using IPv4
  - ➢ connects using IPv6

In this verification, servers were set up to prioritize IPv6 connections to promote migration to IPv6 and it was confirmed that they operated according to made settings.

Evaluation from a Building Standpoint

IPv6 compliant servers and network devices are on the increase. This verification made use of IPv4/IPv6 dual stack compliant equipment. However, use of IPv6 multicast (PIM-SM) and IPv6 automatic RouterAdvertise (RA) and other functions caused some devices (switches and wireless LAN access point cell stations) to drop or block packets or otherwise not operate normally. Feedback generated by the verification have resulted in firmware updates and improvements in operation, but building the new system has not been smooth and the migration process will take more time than initially expected.

Since both the current IPv4 addresses and IPv6 addresses had to be included in the design of the system, the workload of the staff during the migration period has been anything but light.

Evaluation from an Operator Standpoint

The implementation of IPv6 will see the connection of a vast number of network devices. So far the management of remote equipment (routers) such as installing, setting up and checking had to be performed locally either by the administrator (builder) or by local employees. The management framework of being able to set up and maintain equipment settings in the center server will become all the more important in the migration to IPv6. We have established that in the event of equipment failure it will be possible for local employees without any knowledge of the device to plug in a new device sent by the provider and the settings for the replaced device in the center server can be used in setting up the new device. As a result, this management framework will reduce the amount of work required. This type of management technique will become indispensable in managing the vast number of devices that will be connected in the migration to IPv6.

Evaluation from a User Standpoint

Since it has been established that the user will not need to be make any terminal settings in the migration from IPv4 to IPv6 to connect to the network, the burden on the user is expected to be light. It has been established that IPv4 native terminals and IPv6 native terminals will both be capable of accessing IPv4 and IPv6 services so the regular user will not need to bother with any of the following issues.

- The use of an IPv4 terminal excludes access to an IPv6 service.
- A change to IPv6 will excludes access to an existing IPv4 service.

Evaluation of IPv6 Deployment Costs

This time only equipment to make the Internet connection IPv6 compliant and translator devices to enable services between the two systems have been installed. Otherwise a dual stack approach has been implemented assigning IPv6 addresses to all devices to preclude the need for installing new devices.

Evaluation of the IPv6 Deployment Process

This is an evaluation of the points listed in the deployment scenario.

- There are no changes to the existing IPv4 access method.

It has been established that existing IPv4 terminals will be able to use the IEEE802.11a/b/g/ wireless LAN access system even after the wireless LAN access point system migrates to IPv6. Internet access has been confirmed and connections to the network environment will go through IEEE802.1x PEAP authentication and automatic address assignment via DHCP. This indicates that there is no change to the existing IPv4 access system.

- IPv6 deployment will not change the access system.

In the connection of a regular user IPv4 terminal to the Internet, DHCP automatically assigns an IP address to the client and there is no need to bother about network settings. After migrating to IPv6, addresses will also be automatically assigned in the same way and will not require any user settings. Since the IPv6 environment enables connection using SSID and 802.1x, there is again no need for regular users to make any settings. Thus IPv6 deployment does not involve any changes in the access system.

- Access from existing IPv4 of IPv6 services will be possible.

It has been established that with the use of translators existing IPv4 terminals can access IPv6 sites so there is no need to upgrade to an IPv6 terminal to access IPv6 services.

- Regular users and service providers should be able to maintain the connectivity of the existing environment also after migration to IPv6.

It has been confirmed that regular user terminals even after migration to IPv6 will be able to access existing IPv4 sites using translators after the provider migrates to IPv6. Thus connectivity to the existing environment after IPv6 deployment is confirmed for both users and providers.

Thus the viability of the deployment scenario for the wireless LAN access point system has been vindicated.

Tips

(1) Multicast

Multicast transmission could not be performed since multicast with CiscoCatalyst resulted in dropped packets. The ICMPv6 multicast listener report to DR did not arrive due to dropped packets and a Join message was as a result not issued. This issue is now being negotiated with the vendor.

6.3.4 Issues

This section describes the problems that occurred in migration to IPv6 according to the model presented here.

Issues

(1) Mobile IPv6

When a terminal moves to a different access point, a new address must normally be obtained from the previous address. This is because each wireless access point is independent, the network is split into subnetworks and the prefix addresses differ. Since an address change means that TCP/UDP are temporarily disconnected, transmission is also temporarily interrupted. In IPv6, connectivity in going between wireless LAN access points for mobile IPv6 transmission will be maintained, but this has not actually been verified.

Future Outlook

(1) Mobile IPv6

Currently, specifications to expand protocols to maintain connectivity to the network transparently during movement between access points in a wireless LAN environment under RFC2002 have been presented. RFC2002 will become the standard for IPv6 for mobile IP specifications and is expected to be implemented in standard devices in the near future.

7. Guideline for ISP Segment

7.1 Overview

This chapter discusses guidelines for small- and medium-sized Internet service providers (ISP) to migrate to IPv6. In Part 2, we build an actual model ISP as a case study to examine the solution implemented when migrating from IPv4 to IPv6, as well as the advantages and issues that arose from this migration. Although the scope in Part 2 focuses on small- and medium-sized ISPs, it also encompasses an outlook that includes large ISPs and corporate networks.

7.2 Typical Deployment Scenarios for Networks of Small- and Medium-sized ISPs

Referring to the guidelines put out by the IPv6 Promotion Council DP-WG Guideline Deployment Working Group (hereinafter referred to as the "Deployment WG Guidelines"), we are providing the following systems as examples for typical migration scenarios for networks of small- and medium-sized ISPs.

The deployment scenarios discussed here cite examples whereby the subsystems constituting an ISP network are taken apart, and each subsystem is subjected to several scenarios. When performing the actual deployment, the most appropriate method was chosen from among these typical scenarios, or from among other atypical scenarios, taking into account the particular conditions and characteristics of each ISP network.

7.2.1 Prior to IPv6 Deployment

Figure 7.2.1.1 shows a typical example of a legacy configuration before a small- and medium-sized ISP network is migrated to IPv6.

The network in this example is made up of four subsystems: the access subsystem, the backbone subsystem, the upstream connection subsystem, and the server subsystem. These all provide only IPv4 services. (Note that, in reality, the upstream connection subsystem often includes peering and other types of connectivity; in the interests of simplicity, Part 2 discusses a simple upstream connection.)

Note that, although there are many cases that do not follow this example, such as when the access and backbone subsystems are difficult to differentiate in a small- or medium-sized ISP, or when the access and server subsystems have been outsourced to an outside service provider, to handle all the cases, the following scenarios all assume that the ISP provides all these subsystem services.

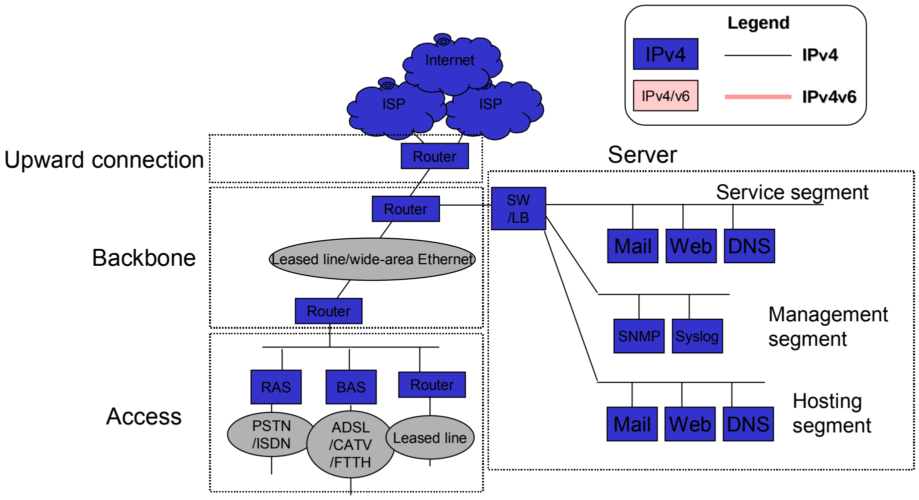


Figure 7.2.1.1: Typical ISP Configuration Example

7.2.2 IPv6 Deployment Scenario (upstream connection)

In this section, the IPv6 installation methods for this scenario are classified into three major approaches. Figure 7.2.2.1 depicts the first method.

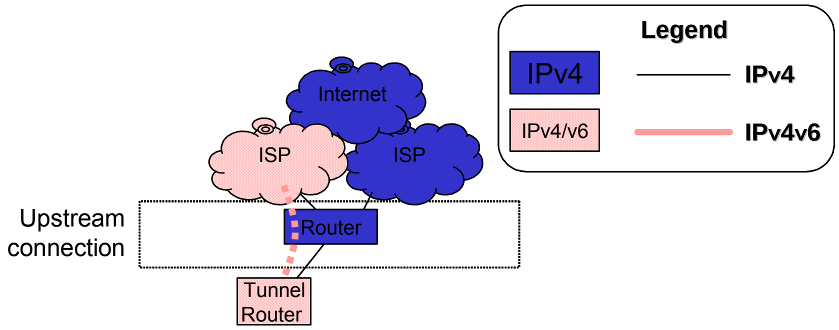


Figure 7.2.2.1: Upstream Connection Deployment Scenario 1

This method to provide support for IPv6 corresponds to a system that is referred to by the Deployment WG Guidelines as "tunneling." With this method, a new tunnel router is set up at any point in the network, and IPv6 over IPv4 is used to establish an indirect connection to the upstream ISP via an IPv4 network.

Advantages provided by this approach include the ability to easily extend IPv6 networks to areas in which it is needed, due to the fact that little change to the existing network configuration is needed, the ability to maintain the stability of the existing IPv4 network, and the ability to hold down costs of installing new equipment due to the fact that when newly introducing a tunnel router it is possible to use an IPv6 router that is already being used for other purposes. However, the use of tunneling has its own inherent issues (such as decreases in MTU and constraints on the tunneling transfer functionality), and so may cause other problems.

Figure 7.2.2.2 depicts the second method.

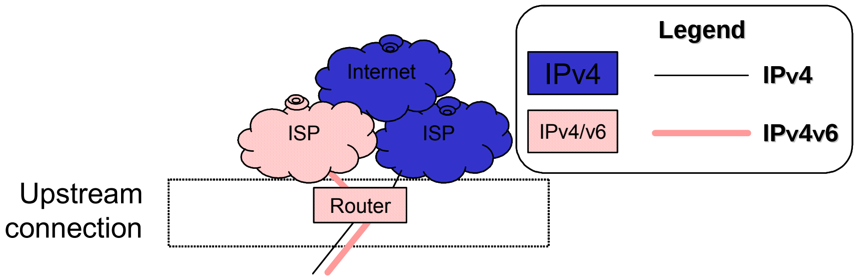


Figure 7.2.2.2: Upstream Connection Deployment Scenario 2

This method to provide support for IPv6 corresponds to a system that is referred to by the Deployment WG Guidelines as "dual." With this method, the operating system of an existing IPv4 upstream connection router is replaced and the router is set up to provide a dual stack. This method enables the router to be used to implement an IPv6 upstream connection and accommodate the existing IPv4 upstream connection.

Advantages provided by this approach include the ability to implement an IPv6 upstream connection using existing equipment, thus incurring little cost. However, a concern is that configuring dual stack devices in which only IPv4 has been set may adversely affect the operating stability of the IPv4 unit, so adequate operation tests must be performed before implementation.

Figure 7.2.2.3 depicts the third method.

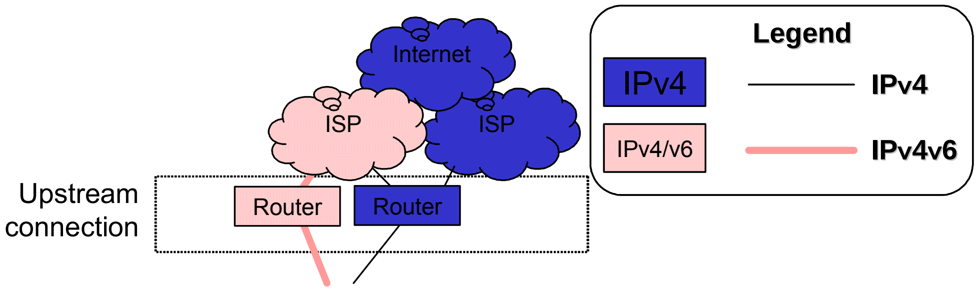


Figure 7.2.2.3: Upstream Connection Deployment Scenario 3

With this method, a new IPv6 upstream connection router is installed in parallel with the existing IPv4 upstream connection router. Not only can the IPv6 router be used for dedicated IPv6 connections, it can also be configured to perform IPv4 connections in order to gain redundancy for IPv4 upstream connections. (The former case corresponds to a system referred to by the Deployment WG Guidelines as "native," and the latter case corresponds to a system referred to as "dual.")

Advantages provided by this approach include the ability to implement an IPv6 upstream connection while maintaining the configuration and stability of the existing IPv4 upstream connections. However, the tradeoff is an increase in costs associated with installing, managing and maintaining the new equipment.

7.2.3 IPv6 Deployment Scenario (Backbone)

In this section, the IPv6 installation methods for this scenario are classified into three major approaches. Figure 7.2.3.1 depicts the first method.

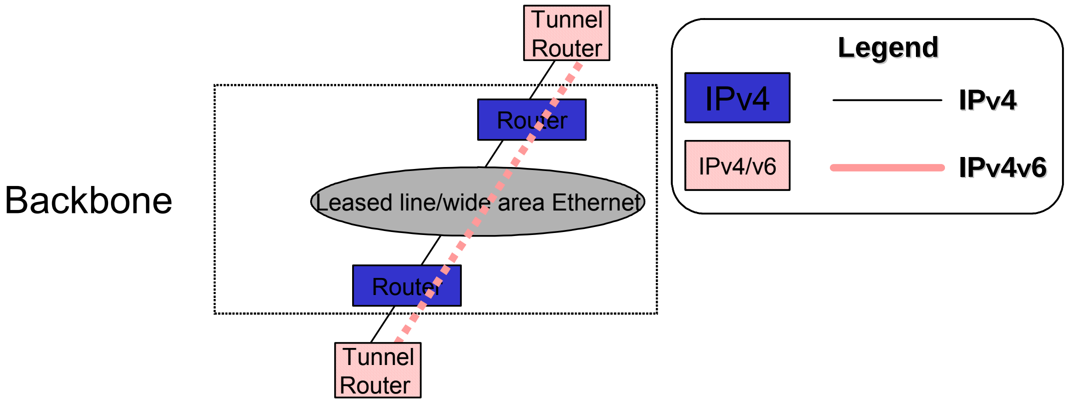


Figure 7.2.3.1: Backbone Migration Method 1

This method to provide support for IPv6 corresponds to a system that is referred to by the Deployment WG Guidelines as "tunneling." With this method, an IPv6 over IPv4 tunnel can be set up to bypass the IPv4 backbone without changing the existing IPv4 backbone configuration.

Similar to the case of upstream connection migration method 1, the advantages of this approach include the ability to maintain the stability of the existing backbone and to hold down new installation costs. However, the use of tunneling has its own inherent issues and so may cause other problems.

Figure 7.2.3.2 depicts the second method.

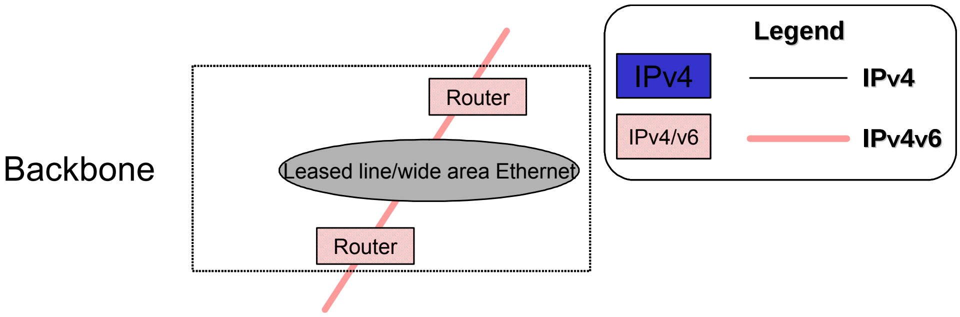


Figure 7.2.3.2: Backbone Migration Method 2

This method to provide support for IPv6 corresponds to a system that is referred to by the Deployment WG Guidelines as "dual." With this method, a dual stack router can be set up by replacing the OS used for the existing IPv4 backbone router. This method allows the router to be used to implement an IPv6 backbone connection and accommodate the existing IPv4 backbone connection as well.

Similar to the case of upstream connection migration method 2, the advantages of this approach include the ability to implement an IPv6 backbone connection using existing equipment at little cost. However, a concern is that this approach may adversely affect IPv4 performance and operating stability.

Figure 7.2.3.3 depicts the third method.

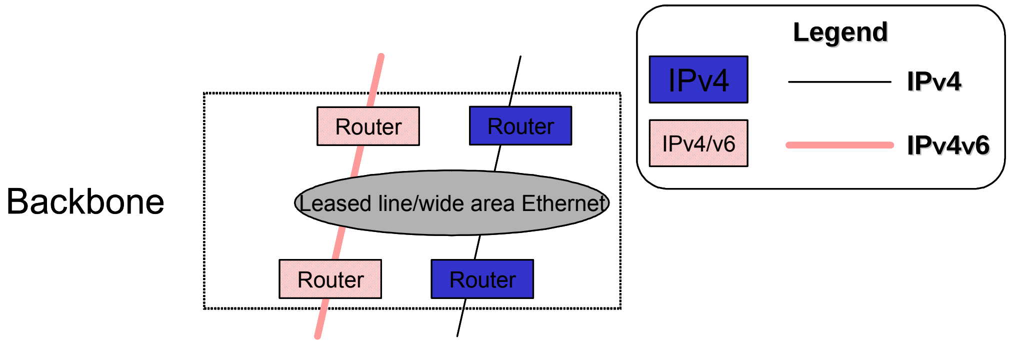


Figure 7.2.3.3: Backbone Migration Method 3

With this method, a new IPv6 backbone router is installed in parallel with the existing IPv4 backbone router. Not only can the IPv6 router be used for dedicated IPv6 connections, it can also be configured to perform IPv4 connections in order to gain redundancy for IPv4 backbone connections. (The former case corresponds to a system referred to by the Deployment WG Guidelines as "native," and the latter case corresponds to a system referred to as "dual.")

Similar to the case of upstream connection migration method 3, the advantages of this approach include the ability to implement an IPv6 backbone connection while maintaining the configuration and stability of the existing IPv4 backbone connection. However, the tradeoff is an increase in costs associated with installing, managing and maintaining the new equipment.

7.2.4 IPv6 Deployment Scenario (Access)

In this section, the IPv6 installation methods for this scenario are classified into three major approaches. Figure 7.2.4.1 depicts the first method.

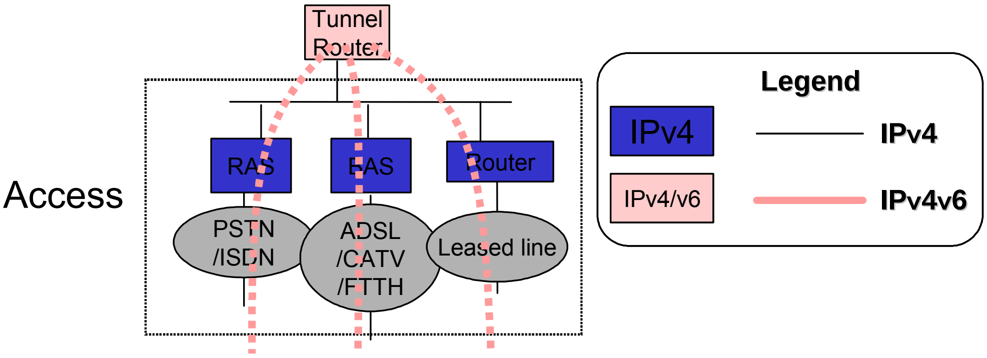


Figure 7.2.4.1: Access Migration Method 1

This method to provide support for IPv6 corresponds to a system that is referred to by the Deployment WG Guidelines as "tunneling." With this method, an IPv6 over IPv4 tunnel is set up between a tunnel router and the end users without changing the existing IPv4 access system configuration.

Similar to the case of upstream connection migration method 1, the advantages of this approach include the ability to maintain the stability of the existing access connections and to hold down new installation costs thanks to the shared use of equipment. However, the use of tunneling has its own inherent issues and so may cause other problems.

Figure 7.2.4.2 depicts the second method.

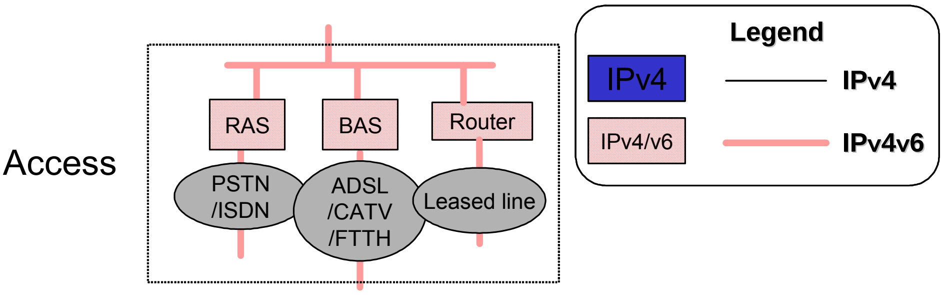


Figure 7.2.4.2: Access Migration Method 2

This method to provide support for IPv6 corresponds to a system that is referred to by the Deployment WG Guidelines as "dual." With this method, a dual stack router can be set up by replacing the OS used for the existing IPv4 access router. This method allows the use of a router to implement an IPv6 backbone connection and accommodate existing IPv4 access.

Similar to the case of upstream connection migration method 2, the advantages of this approach include the ability to implement an IPv6 backbone connection using existing equipment, thus incurring little cost. However, a concern is that this approach may adversely affect IPv4 performance and operating stability.

Figure 7.2.4.3 depicts the third method.

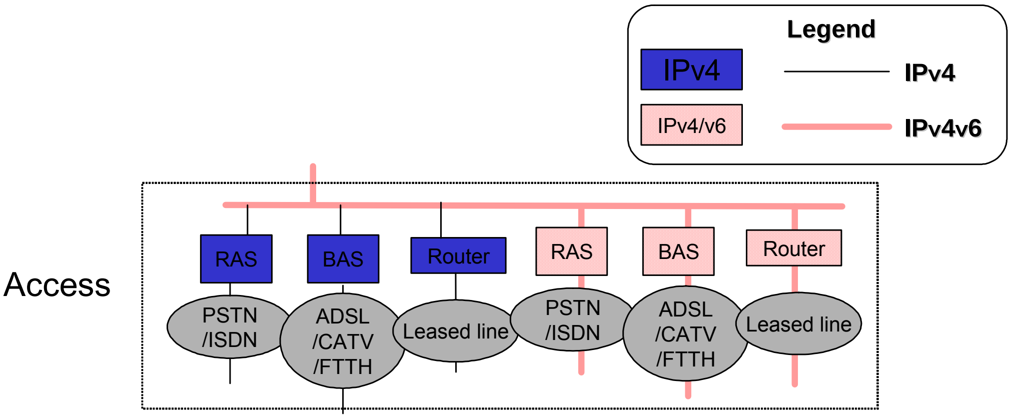


Figure 7.2.4.3: Access Migration Method 3

With this method, a new IPv6 access router is installed in parallel with the existing IPv4 access router. For access connections, there are undoubtedly numerous cases in which the router accommodates not only IPv6, but also IPv4 at the same time. (The former case corresponds to a system referred to by the Deployment WG Guidelines as "native," and the latter case corresponds to a system referred to as "dual.")

Similar to the case of upstream connection migration method 3, the advantages of this approach include the ability to implement an IPv6 access connection while maintaining the configuration and stability of the existing IPv4 access connection. However, in addition to the costs associated with installing, managing and maintaining new equipment, depending on the configuration, the user or access provider may need to reconfigure network devices when implementing the IPv6 connection, which may result in communication outages.

7.2.5 IPv6 Deployment Scenario (Server)

In this section, the IPv6 installation methods for this scenario are classified into two major approaches. Figure 7.2.5.1 depicts the first method.

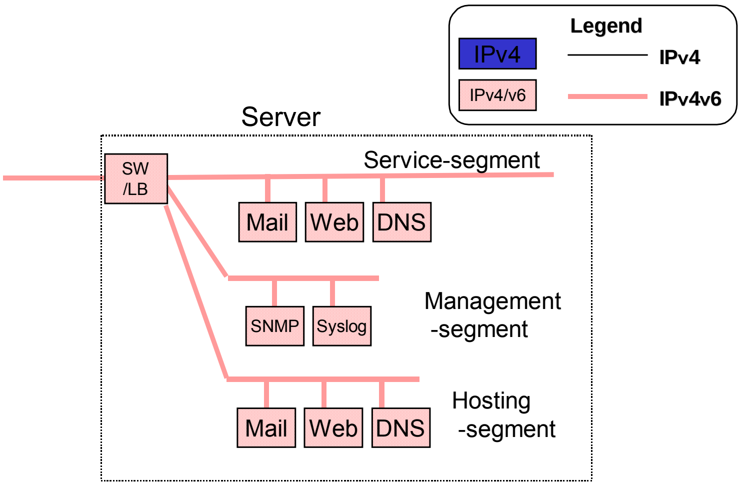


Figure 7.2.5.1: Server Migration Method 1

With this method, the operating system and applications of the existing IPv4 server are replaced and a dual stack server is set up. This method allows the server to implement both IPv6 services and existing IPv4 services.

The advantages of this approach include the ability to provide IPv6 server services using existing equipment, thus incurring little cost. However, a concern is that this approach may adversely affect the operating stability of the IPv4 unit.

Figure 7.2.5.2 depicts the second method.

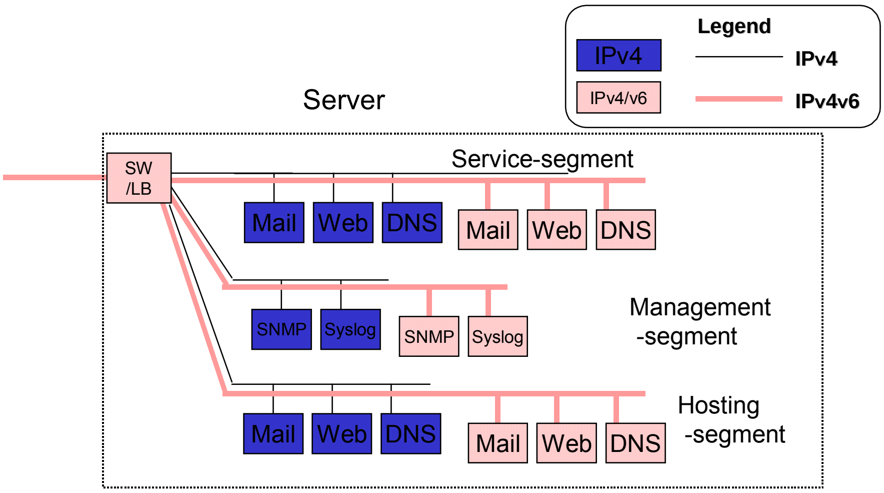


Figure 7.2.5.2: Server Migration Method 2

With this method, a dual stack server is installed in parallel with the existing IPv4 server. At the application level, the dual stack server is configured to operate in coordination with the existing IPv4 server. If needed, the dual stack server can be used to provide redundancy services for the existing IPv4 server.

Advantages provided by this approach include the ability to provide IPv6 server services while maintaining the configuration and stability of the existing IPv4 server services. However, in addition to the increases costs associated with installing, managing and maintaining new equipment, one must determine how to configure the IPv6 server to work together with the existing IPv4 server.

7.3 Actual Case Study

Assuming a model case of a small- and medium-sized ISP, Part 2 compiles a case study examining and evaluating an actual implementation of IPv6 in that ISP.

The following sections refer to a model case of the ISP selected for Part 2.

7.3.1 Model Case

The following provides an outline of the ISP selected as the model case in Part 2.

To consider a migration scenario in which coverage is maintained over a wide area, the model selected here assumes a relatively large small- and medium-sized ISP having several tens of thousands of end users and an ample redundancy network configuration. Regarding user access, it is assumed that the general user mainly connects using ADSL via an access provider, and that relatively large business users connect via carrier-provided wide-area Ethernet services.

The network configuration is implemented using a two NOC configuration. NOC-A provides the user connection and NOC-B is used to implement the upstream connection. FastEthernet connections are used to simulate carrier wide-area Ethernet service between the NOCs comprising the network core subsystem.

For the upstream connection, NTT/VERIO IPv4 transit service is used and a redundant connection configuration is implemented based on BGP using two dedicated upstream connection routers. At the same time, IPv4 addresses are allocated by NTT/VERIO.

In addition to an ISP's public access Web, DNS and mail servers, the server farm includes NMS and other management servers. A firewall is provided to protect portions of the server farm and provide security for customers using housing services.

The access subsystem is made up of an Ethernet switch and an IPv4 router. In addition to concentrating general users connecting via an access provider, in this configuration the Ethernet switch can also be used to provide private line connections to business users. Note that, in general, ADSL is implemented with access provider equipment. Since this means that providing support for IPv6 by the access provider means migrating ADSL to IPv6, this falls outside the scope of ISP migration discussed in Part 2. Dial-up and television-based connections are also not considered in this migration scenario. With respect to dial-up, permanent connections will soon be the norm and there are too few TV-based connections to consider them in the context of a model case.

Physical Network Configuration

Figure 7.3.1.1 depicts the overall network physical configuration of the model case discussed in Part 2.

NOC-A mainly includes equipment for access and for connecting to the backbone, as well as the server farm. NOC-B includes upstream connection equipment and backbone connection equipment. It is assumed that, between the two NOCs, there is a connection that uses wide-area Ethernet service in place.

The following pages detail the configuration of each NOC.

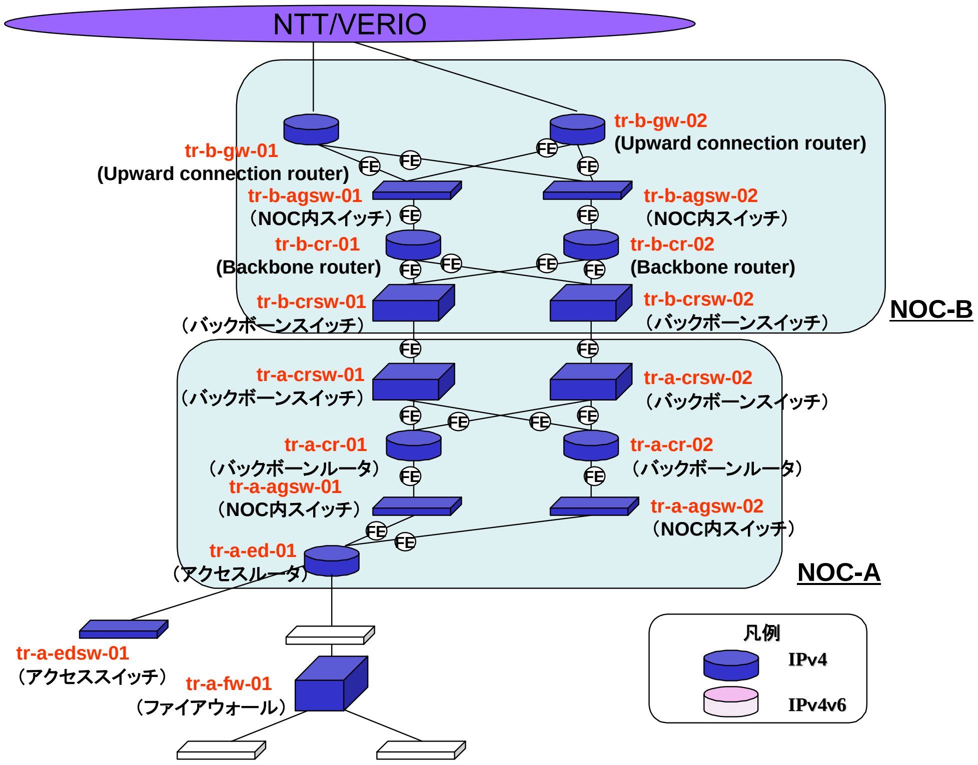


Figure 7.3.1.1: Network Physical Configuration (before Migration)

(1) NOC-B

NOC-B is configured with two upstream connection gateway routers and, including the redundancy system, two core routers for connecting to the backbone. The NOC internal and backbone connectivity is implemented with an Ethernet network and switches are set up for these connections.

Table 7.3.1.1 shows the products used to configure NOC-B.

Table 7.3.1.1: Products Making Up NOC-B

No.	Host	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	tr-b-cr-01	Juniper M5	JUNOS 6.1R5	fe-0/0/0	tr-b-agsw-01	fastethernet-0/10	FastEthernet	Backbone router
				fe-0/0/1	tr-b-crsw-01	e1	FastEthernet	
				fe-0/0/2	tr-b-crsw-02	e2	FastEthernet	
2	tr-b-cr-02	CISCO 12404IR	IOS12.0(26)S	fastethernet-1/0	tr-b-agsw-02	fastethernet-0/10	FastEthernet	Backbone router
				fastethernet-1/1	tr-b-crsw-01	e1	FastEthernet	
				fastethernet-1/2	tr-b-crsw-02	e2	FastEthernet	
5	tr-b-gw-01	CISCO 7204VXR	IOS12.2(15)T	gigabitethernet-0/1	(NTT/VERIO)		FastEthernet	Upstream connection router
				gigabitethernet-0/2	tr-b-agsw-01	fastethernet-0/1	FastEthernet	
				gigabitethernet-0/3	tr-b-agsw-02	fastethenret-0/2	FastEthernet	
6	tr-b-gw-02	Juniper M5	JUNOS 6.1R5	fe-0/0/1	tr-b-agsw-01	fastethernet-0/1	FastEthernet	Upstream connection router
				fe-0/0/2	tr-b-agsw-02	fastethernet-0/2	FastEthernet	
				fe-0/0/3	(NTT/VERIO)		FastEthernet	
114	tr-b-crsw-01	Foundry FastIron2402	03.0.00Tc1	e1	tr-b-cr-01	fe-0/0/1	FastEthernet	Backbone switch
				e2	tr-b-cr-02	fastethernet-1/1	FastEthernet	
				e10	tr-a-crsw-01	e10	FastEthernet	
118	tr-b-crsw-02	Foundry FastIron2402	03.0.00Tc1	e1	tr-b-cr-01	fe-0/0/2	FastEthernet	Backbone switch
				e2	tr-b-cr-02	fastethernet-1/2	FastEthernet	
				e10	tr-a-crsw-02	e10	FastEthernet	
98	tr-b-agsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-b-gw-01	gigabitethernet-0/2	FastEthernet	NOC internal switch
				fastethernet-0/2	tr-b-gw-02	fe-0/0/1	FastEthernet	
				fastethernet-0/10	tr-b-cr-01	fe-0/0/0	FastEthernet	
106	tr-b-agsw-02	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-b-gw-01	gigabitethernet-0/3	FastEthernet	NOC internal switch
				fastethernet-0/2	tr-b-gw-02	fe-0/0/2	FastEthernet	
				fastethernet-0/10	tr-b-cr-02	fe-0/0/0	FastEthernet	

(2) NOC-A

NOC-A is configured with a single access edge router and, including the redundancy system, two core routers for connecting to the backbone. A server farm is also located below NOC-A and, as with NOC-B, the NOC internal and backbone connectivity is implemented with an Ethernet network and switches are set up for these connections.

Table 7.3.1.2 shows the products used to configure NOC-A.

Table 7.3.1.2: Products Making Up NOC-A

No.	Host	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	tr-a-cr-01	Juniper M5	JUNOS 6.1R5	fe-0/0/0	tr-a-gsw-01	fastethernet-0/10	FastEthernet	Backbone router
				fe-0/0/1	tr-a-crsw-01	e1	FastEthernet	
				fe-0/0/2	tr-a-crsw-02	e2	FastEthernet	
2	tr-a-cr-02	CISCO 12404IR	IOS12.0(26)S	fastethernet-1/0	tr-a-agsw-02	fastethernet-0/10	FastEthernet	Backbone router
				fastethernet-1/1	tr-a-crsw-01	e1	FastEthernet	
				fastethernet-1/2	tr-a-crsw-02	e2	FastEthernet	
9	tr-a-ed-01	CISCO 7204VXR	IOS12.2(15)T	gigabitethernet-0/1	tr-a-edsw-01	fastethernet-0/1	FastEthernet	Access router
				gigabitethernet-0/2	tr-b-agsw-01	fastethernet-0/1	FastEthernet	
				gigabitethernet-0/3	tr-b-agsw-02	fastethenret-0/2	FastEthernet	
				fastethernet-2/0	HUB (HUB-v4-1)		FastEthernet	
146	tr-a-crsw-01	Foundry FastIron2402	03.0.00Tc1	e1	tr-a-cr-01	fe-0/0/1	FastEthernet	Backbone switch
				e2	tr-a-cr-02	fastethernet-1/1	FastEthernet	
				e10	tr-b-crsw-01	e10	FastEthernet	
150	tr-a-crsw-02	Foundry FastIron2402	03.0.00Tc1	e1	tr-a-cr-01	fe-0/0/2	FastEthernet	Backbone switch
				e2	tr-a-cr-02	fastethernet-1/2	FastEthernet	
				e10	tr-b-crsw-02	e10	FastEthernet	
130	tr-a-agsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-01	gigabitethernet-0/2	FastEthernet	NOC internal switch
				fastethernet-0/10	tr-a-cr-01	fe-0/0/0	FastEthernet	
138	tr-a-agsw-02	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-01	gigabitethernet-0/3	FastEthernet	NOC internal switch
				fastethernet-0/10	tr-a-cr-02	fe-0/0/0	FastEthernet	
154	tr-a-edsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-01	gigabitethernet-0/1	FastEthernet	Access switch

(3) Servers

Figure 7.3.1.2 depicts the configuration of the server farm and Table 7.3.1.3 lists the products used to configure it.

A single firewall is placed under NOC-A and several servers are located outside and inside the firewall.

A single public Web server and two combination public mail/DNS servers are configured outside the firewall. Inside the firewall, a single combination DNS/mail server is set up for use by ISP users and internal operators.

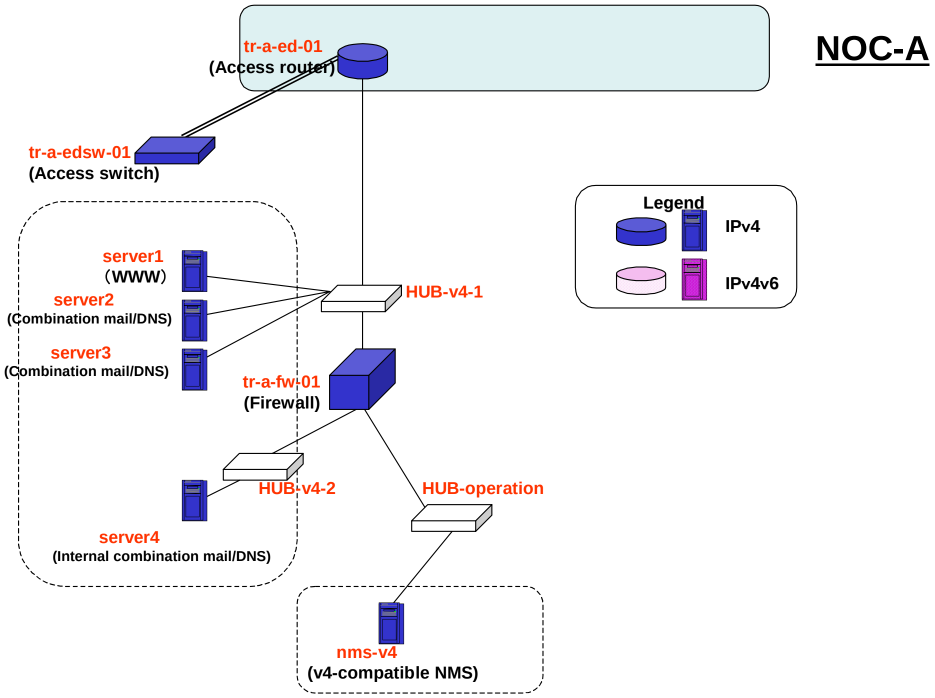


Figure 7.3.1.2: Physical Configuration of Servers (before Migration)

Table 7.3.1.3: Products Making Up Servers

No.	Host	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
13	tr-a-fw-01	NOKIA-IP380	IPSO 3.7 FireWall-1 4.1	eth1	HUB (HUB-v4-1)		FastEthernet	Firewall
				eth2	HUB (operation)		FastEthernet	
				eth3	HUB (HUB-v4-2)		FastEthernet	
195	server1	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Web server
196	server2	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Combination public mail/DNS server
197	server3	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Combination public mail/DNS server
202	server4	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-2)		FastEthernet	Internal combination mail/DNS server
244	nms-v4	SunBlade 150	Solaris 9	eri0	HUB (operation)		FastEthernet	NMS server

Logical Network Configuration

This subsection describes the logical configuration of the network for the model case ISP.

The following describes the configurations of Layer 2 (Ethernet layer) and Layer 3 (IP layer).

(1) Configuration of Layer 2

Figure 7.3.1.3 depicts the configuration of Layer 2 in NOC-B and NOC-A. FastEthernet is used within the NOCs, and VLAN is used as needed. The circled numbers in the figure indicate the VLAN number.

In addition to the segments for normal traffic, segments for backup and management are also in place, with segment separation performed by Tag-VLAN.

When users connect, the transmission path first encounters the physical access switch, then tag-VLAN is used to concentrate the logical segments on all access lines onto the link between the access switch and the access router, with the router providing the Layer 3 functions.

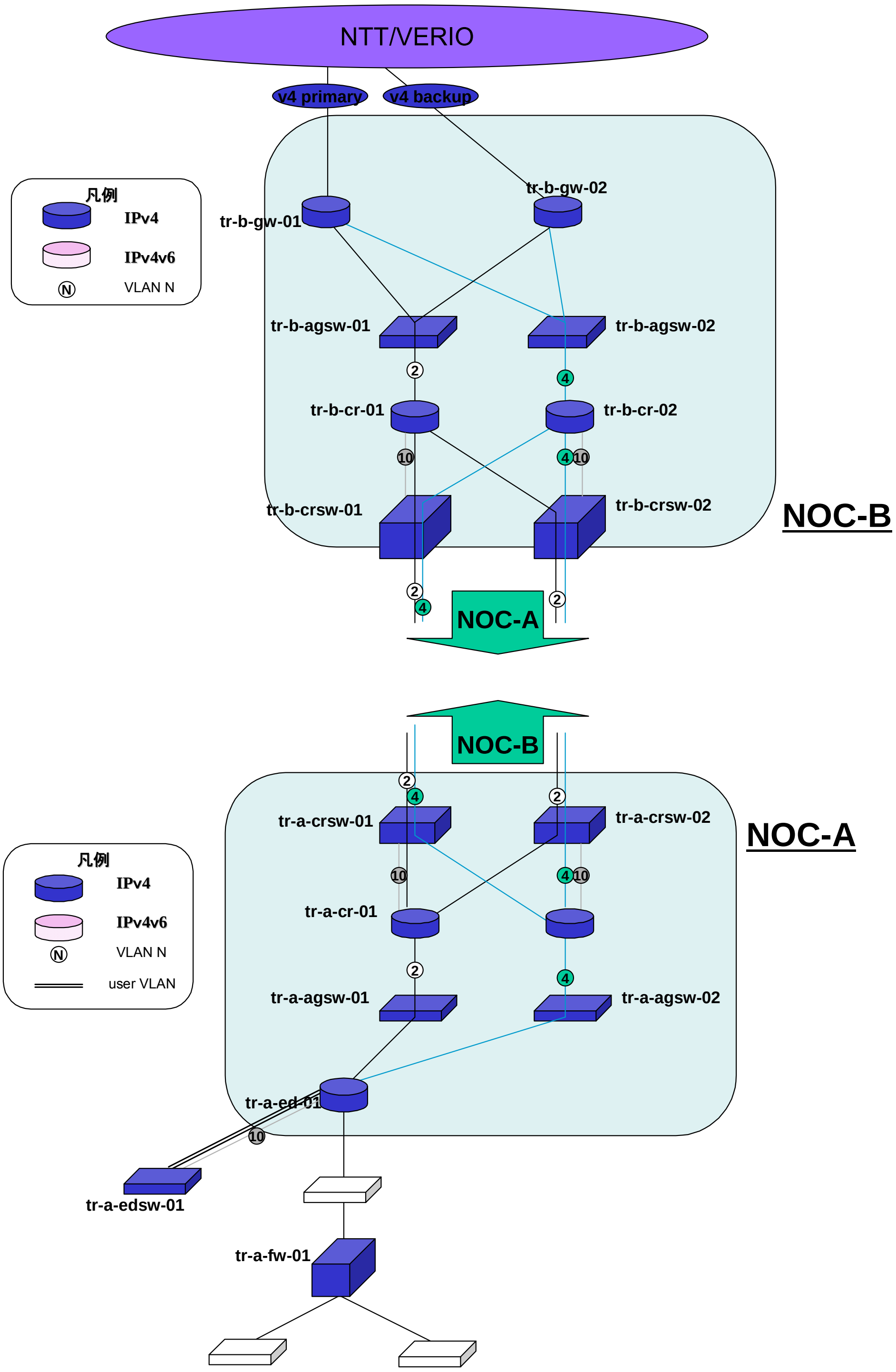


Figure 7.3.1.3: Configuration of Layer 2 (before Migration)

(2) Layer 3 IPv4 topology

Figure 7.3.1.4 depicts the IPv4 Layer 3 topology of the model case ISP.

OSPFv2 is used as the IPv4 routing protocol within the ISP network. The red numbers are the cost of OSPFv2 for the indicated link. (Note that OSPF costs are established manually.)

BGP4 is used as the upstream connection IPv4 routing protocol. For two BGP connections, one side can be used as a dedicated backup by adjusting the BGP attributes.

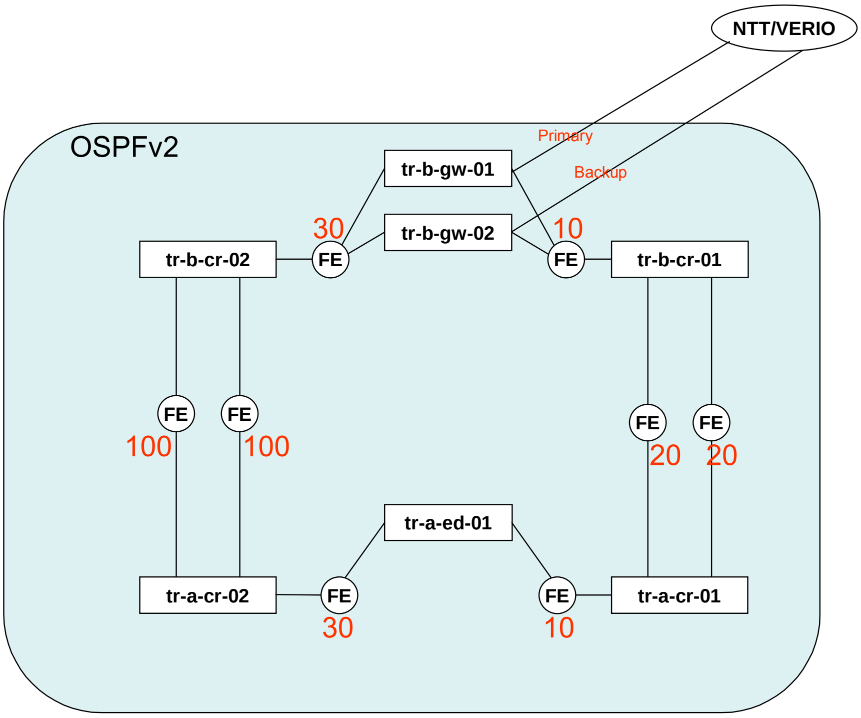


Figure 7.3.1.4: Layer 3 Configuration (before Migration)

Table 7.3.1.4 lists detailed information about IPv4 routing. (In the following, the addresses have been corrected from the actual values.)

Table 7.3.1.4: Routing Information (before Migration)

No.	Host name	Logical interface	Address	OSPFv2 (cost)	BGP Peer	Notes
1	tr-a-cr-01	lo-0	192.0.2.1	ON （1）	no bgp process (default routing)	Backbone router
		fe-0/0/0	192.0.2.129	ON (10)		
		fe-0/0/1.2	192.0.2.65	ON (20)		
		fe-0/0/2	192.0.2.69	ON (20)		
2	tr-a-cr-02	lo-0	192.0.2.2	ON (1)	no bgp process (default routing)	Backbone router
		fastethernet-1/0	192.0.2.137	ON (30)		
		fastethernet-1/1	192.0.2.73	ON (100)		
		fastethernet-1/2.4	192.0.2.77	ON (100)		
3	tr-b-cr-01	lo-0	192.0.2.3	ON （1）	no bgp process (default routing)	Backbone router
		fe-0/0/0	192.0.2.97	ON (10)		
		fe-0/0/1	192.0.2.66	ON (20)		
		fe-0/0/2	192.0.2.70	ON (20)		
4	tr-b-cr-02	lo-0	192.0.2.4	ON (1)	no bgp process (default routing)	Backbone router
		fastethernet-1/0	192.0.2.105	ON (30)		
		fastethernet-1/1	192.0.2.74.	ON (100)		
		fastethernet-1/2	192.0.2.78	ON (100)		
5	tr-b-gw-01	lo-0	192.0.2.5	ON (1)	EBGP NTT/VERIO (AS2914) IBGP tr-b-gw-02 tr-a-ed-01	Upstream connection router
		gigabitethernet-0/2	192.0.2.99	ON (10)		
		gigabitethernet-0/3	192.0.2.107	ON (30)		
6	tr-b-gw-02	lo-0	192.0.2.6	ON (1)	EBGP (export; community 2914:480) (import: LocalPref: 90) NTT/VERIO (AS2914) IBGP tr-b-gw-01 tr-a-ed-01	Upstream connection router
		fe-0/0/1	192.0.2.100	ON (10)		
		fe-0/0/2	192.0.2.108	ON (30)		
9	tr-a-ed-01	lo-0	192.0.2.9	ON (1)	IBGP tr-b-gw-01 tr-b-gw-02	Access router
		gigabitethernet-0/2	192.0.2.131	ON (10)		
		gigabitethernet-0/3	192.0.2.139	ON (30)		
		fastethernet-2/0	192.0.2.193	ON (10)		

Applications

This subsection describes the applications provided by this model case ISP.

The following discusses the configuration of Web, mail and DNS services, which are the main services provided by the ISP in this scenario, as well as the internal ISP management system.

(1) Web

There are two main foci of the service format implemented with the ISP's Web service: information delivery from the ISP and providing Web hosting services to users.

Table 7.3.1.5 shows the actual configuration.

Table 7.3.1.5: Configuration of Web Service (before Migration)

No.	Host name	Specification	OS	Address	Application	Notes
195	server1	HP DL320	FreeBSD4.9	192.0.2.195	apache2.0.48	Web server

In this model case, a single external public Web server has been set up to provide public Web hosting and information.

(2) Mail

The mail service provided by this model case ISP is made up of a total of three servers: two servers for external communications and one server for ISP users and internal operator communications. The MX record of the appropriate zone of the DNS information is used to make one of the two external communication servers the primary server for receiving, and mail addressed to the v6trans.jp domain is delivered to a spool server according to the description in the MX record.

The internal server maintains mail addressed to the v6trans.jp domain in a spool, and provides POP service to its customers. At the same time, the above server is set up to relay mail addressed to external domains in response to a mail transmission request received from a customer.

Table 7.3.1.6 shows the actual configuration.

Table 7.3.1.6: Configuration of Mail Service (before Migration)

No.	Host name	Specification	OS	Address	Application	Notes
196	server2	HP DL320	FreeBSD4.9	192.0.2.196	sendmail8.12.10	Public primary
197	server3	HP DL320	FreeBSD4.9	192.0.2.197	sendmail8.12.10	Public secondary
202	server4	HP DL320	FreeBSD4.9	192.0.2.202	sendmail8.12.10 qpopper 4.0.5	For internal use

Table 7.3.1.7 compiles the mail distribution relationships

Table 7.3.1.7: Mail Distribution Relationship (before Migration)

No.	Host name	Envelope_To	Method	Relay	Notes
196	server2	*	MX		v6trans.jp Primary MX (10)
		v6trans.jp	MailerTable	server4	
197	server3	*	MX		v6trans.jp Secondary MX (20)
202	server4	v6trans.jp	Local		
		*	SmartHost	server2	

(3) DNS

For the DNS service provided by the ISP, this model network maintains the zone information for the v6trans.jp domain and IPv4 reverse DNS lookups; it has two public servers and one cache server for responding to DNS recursive queries to ISP users and internal operators. Note that, in this model, these servers also function as mail servers.

Table 7.3.1.8 shows the actual configuration.

Table 7.3.1.8: Configuration of DNS Service (before Migration)

No.	Host name	Specification	OS	Address	Application	Notes
196	server2	HP DL320	FreeBSD4.9	192.0.2.196	bind8.3.7	Slave v6trans.jp. 2.0.192.in-addr.arpa., etc.
197	server3	HP DL320	FreeBSD4.9	192.0.2.197	bind8.3.7	Zone master v6trans.jp. 2.0.192.in-addr.arpa., etc.
202	server4	HP DL320	FreeBSD4.9	192.0.2.202	bind8.3.7	Cache server

(4) Monitoring system

Table 7.3.1.9 describes the ISP monitoring device.

Using the device listed below, the presence or absence of devices is monitored with PING polling and events are monitored with SNMPtrap.

Table 7.3.1.9: Monitoring Configuration (before Migration)

No.	Host name	Specification	OS	Address	Application	Notes
244	Nms-v4	HP DL320	Solaris9	192.0.2.244	HP OpenView 6.4	

7.3.2 IPv6 Deployment Case Study

This subsection examines a specific IPv6 deployment scenario applicable to the model case ISP described in Section 7.3.1 and derives the advantages and issues of the actual deployment.

IPv6 Deployment Policies

This subsection discusses the deployment policies for migrating the model case ISP to IPv6.

The policies discussed in this subsection are assumed to be deployment policies for a typical small- and medium-sized ISP to migration to IPv6.

(1) Overall policy for migrating to IPv6

The following describes the actual deployment policies for this model case, taking into account the constraints faced by a typical small- or medium-sized ISP.

(a) Minimize effects on existing IPv4 network

For the ISP, provisioning of IP communications is their most important service offering, so the migration to IPv6 must avoid destabilizing IPv4 communications.

Moreover, because the accumulation of experience and operational know-how affect restoration response during failure, a policy that avoids migrating entirely to IPv6 from the initial introduction stage is recommended.

(b) Minimize effects on IPv4 server services

The above also applies to services provided by the servers.

(c) Maintain extensive coverage

To the extent possible, each service should support IPv6. There are, however, exceptions. For example, the IPv6 Deployment WG Guidelines state that, considering the present situation in which anti-virus software does not support IPv6, providing IPv6 mail service is dangerous and is therefore not recommended. However, in Part 2, based on the premise that anti-virus software will also support IPv6 in the near future, we decided to adopt a policy of supporting IPv6 services to the maximum extent possible.

(d) Rationalize introduction costs

It is hoped that the costs to introduce new devices for the described deployment be minimized.

Similarly, for IPv6 network redundancy, a method that takes into account such rationalization efforts during the IPv6 introduction period shall be employed.

(e) Simplify management

An easy-to-understand and manage IPv6 network configuration and IPv6 server service configuration shall be implemented, in order to relieve administrator's workload.

(2) Deployment model applied in this model case

Keeping with the deployment policies described above, this subsection describes a specific IPv6 migration scenario implemented by the model case.

(a) Deployment policies deemed important

Considering maintenance of the wide coverage of the deployment scenario, ensuring the stability of IPv4 communications was deemed to be the most important of the above-described deployment policy requirements and so a deployment scenario suited to this was selected for migration of this model case.

This means that, overall, although it appears that the impact of IPv6 deployment cost is heavy, by adopting the deployment in specific areas only, or possibly by reducing the introduction of new devices as needed, it may be possible to reduce costs.

(b) Migrating the upstream connection subsystem to IPv6

In this model case, there are two IPv4 upstream connection routers arranged in a redundancy configuration, with the backup router not normally being used.

In this scenario, the operating system of this backup router is replaced to enable it to support a dual stack, in which routing for both IPv4 and IPv6 is implemented. (Scenario 2 of 7.2.2 IPv6 Deployment Scenario (upstream connection))

With regard to the existing IPv4 service continuing to provide IPv4 connectivity, this implementation does not compromise the stability of the network as a whole during normal operation. Moreover, when the backup is used due to failure of the device that is normally being used, the system can still provide IPv4 backup connectivity, as it could before the migration. (Although we would rather avoid concurrent use of more than operating system for operations, it was considered unavoidable in keeping with the above considerations.)

Although there are no mandatory issues for implementing IPv6 communications, one IPv6 peering router to connect to other ISPs has already been readied for this model case, providing optimized IPv6 communication with peering on IX or private peering. This router is connected to NTT/VERIO and used for a backup connection for the IPv6 upstream connection.

(c) Migrating the backbone subsystem to IPv6

As with the upstream connection configuration, in this model case, there are two backbone connection routers arranged in a redundancy configuration, with the backup router not being used normally.

In this scenario, the operating system of this backup router is replaced to enable it to support a dual stack, in which routing for both IPv4 and IPv6 is implemented. (Scenario 2 of 7.2.3 IPv6 Deployment Scenario (Backbone))

With regard to the existing IPv4 service continuing to provide IPv4 connectivity, this implementation does not comprise stability of the network as a while during normal operation. Moreover, when the backup is used due to failure of the device that is normally being used, the system can still provide IPv4 backup connectivity, as it could before the migration. It also holds down costs because there is no need to introduce new equipment.

IPv6 communications are implemented using an IPv6 over IPv4 tunnel on the IPv4 backbone connection equipment, which functions as an IPv6 connection backup by using the dual stack equipment described above. Because IPv6 communication can be implemented anywhere IPv4 communication is possible, an advantage here is that there are no additional costs associated with cabling to provision IPv6 connectivity with IPv6 over an IPv4 tunnel. (Scenario 1 of 7.2.3 IPv6 Deployment Scenario (Backbone))

(d) Migrating the access subsystem to IPv6

In this model case, there is one router acting as the access subsystem before migration. The access subsystem is not arranged in a primary, backup configuration.

In this scenario, a new dual stack router that enables IPv6 access is readied, and IPv6 support is implemented such that it does not affect the existing access. (Scenario 3 of 7.2.4 IPv6 Deployment Scenario (Access))

Two methods for providing IPv6 connection between private line users and the ISP are assumed: In addition to implementing it by means of a dual stack via a single user line, IPv6 can be provided natively using VLAN or another line.

As mentioned earlier, this scenario does not consider migration of ADSL and other DSL connection services that could be offered because the ISP provider purchases it from the access provider.

(e) Migrating the server subsystem to IPv6

In this scenario, a new dual stack segment is readied behind the new dual stack routers installed for migrating the access subsystem to IPv6, and a dual stack server is installed in this segment. A new dual stack firewall is provided in this segment and, similarly, a dual stack server segment is provided behind this. This ensures that the IPv6-compliant segment will not affect the existing IPv4 server segment. By installing a new IPv6-compliant server in this segment, IPv6 server services can be provided without affecting the existing IPv4 server services. (Scenario 2 of 7.2.5 IPv6 Deployment Scenario (Server))

(f) Summary

Referring to Section 7.2, Table 7.3.2.1 summarizes the migration scenarios that we plan to adopt.

Table 7.3.2.1: Adopted Deployment Scenarios

No.	Subsystem	Scenario	Notes
1	Upstream connection	Scenario 2	Uses available redundancy router
2	Backbone	Scenario 2 (and scenario 1)	Uses available redundancy router
3	Access	Scenario 3	Stresses IPv4 communications stability
4	Server	Scenario 2	Stresses IPv4 service stability

Physical Network Configuration

Figure 7.3.2.1 depicts the configuration after the model case discussed in Part 2 has been migrated to IPv6. In addition to providing a dual stack in one of the backbone connection routers and one of the upstream connection routers, a number of new dual stack routers have been installed.

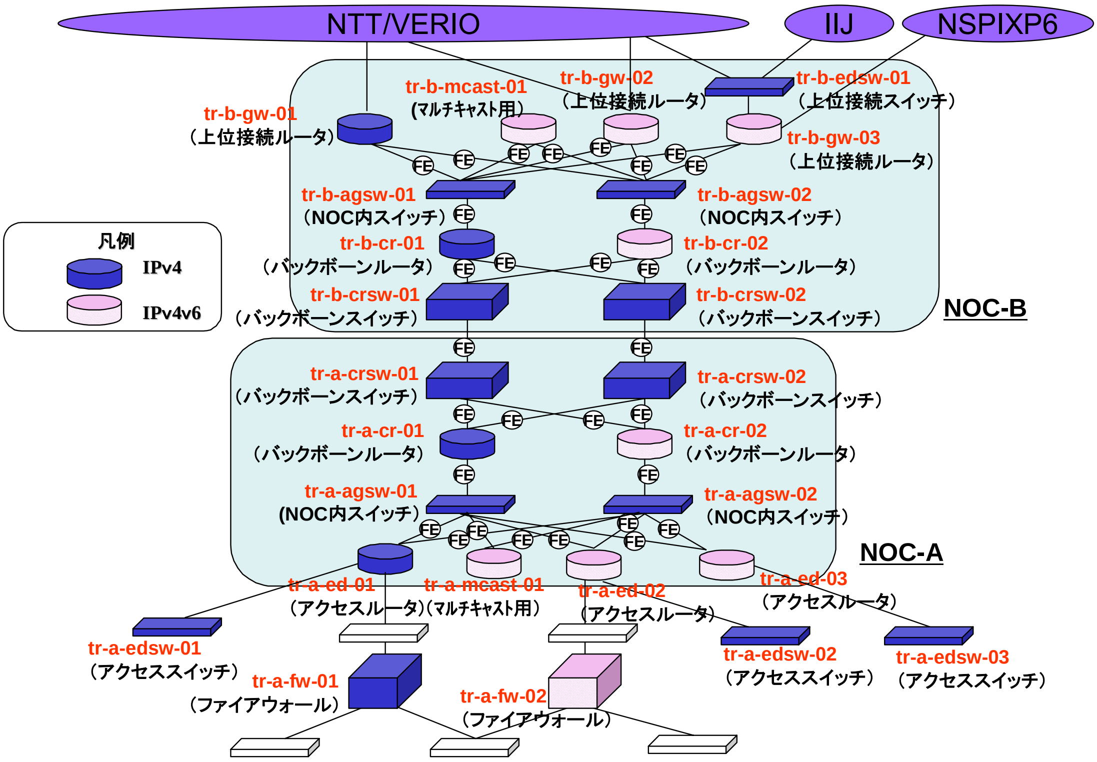


Figure 7.3.2.1: Physical Configuration of Network (after Migration)

(1) NOC-B

The router being used to back up the IPv4 upstream connection is changed to a dual stack device and serves as the primary IPv6 connection, handling BGP connections with NTT/VERIO.

Another dual stack router is installed for IPv6 backup to provide redundancy for the IPv6 BGP upstream connection. This router is also used for peering and performs private peering with the wireless LAN access segment and peering with NSPIXP6. (The network indicated by "IIJ" in the network configuration figure is a wireless LAN access segment for which IIJ is conducting testing.)

One dual stack router is installed between the NOCs for IPv6 backbone communications. This router also performs the role of a backup router for IPv4 backbone communications.

In addition to the above, a separate IPv6 multicast router is installed to perform stable, IPv6 multicast communications.

Table 7.3.2.2 lists the products that make up NOC-B.

Table 7.3.2.2: Products Making Up NOC-B

No.	Host name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	tr-b-cr-01	Juniper M5	JUNOS 6.1R5	fe-0/0/0	tr-b-agsw-01	fastethernet-0/10	FastEthernet	Backbone router
				fe-0/0/1	tr-b-crsw-01	e1	FastEthernet	
				fe-0/0/2	tr-b-crsw-02	e2	FastEthernet	
2	tr-b-cr-02	CISCO 12404IR	IOS12.0(26)S	fastethernet-1/0	tr-b-agsw-02	fastethernet-0/10	FastEthernet	Backbone router
				fastethernet-1/1	tr-b-crsw-01	e1	FastEthernet	
				fastethernet-1/2	tr-b-crsw-02	e2	FastEthernet	
5	tr-b-gw-01	CISCO 7204VXR	IOS12.2(15)T	gigabitethernet-0/1	(NTT/VERIO)		FastEthernet	Upstream connection router
				gigabitethernet-0/2	tr-b-agsw-01	fastethernet-0/1	FastEthernet	
				gigabitethernet-0/3	tr-b-agsw-02	fastethenret-0/2	FastEthernet	
6	tr-b-gw-02	Juniper M5	JUNOS 6.1R5	fe-0/0/1	tr-b-agsw-01	fastethernet-0/1	FastEthernet	Upstream connection router
				fe-0/0/2	tr-b-agsw-02	fastethernet-0/2	FastEthernet	
				fe-0/0/3	(NTT?VERIO)		FastEthernet	
7	tr-b-gw-03	GR2000-2B+	ROUTE-OS7B	fastethernet-0	(NSPIXP6)		FastEthernet	Upstream connection router
				fastethernet-1	tr-b-agsw-01	fastethernet-0/3	FastEthernet	
				fastethernet-2	tr-b-agsw-02	fastethernet-0/3	FastEthernet	
				fastethernet-3	tr-b-edsw-01	fastethernet-0/1	FastEthernet	
8	tr-b-mcast-01	HP DL360 G2	FreeBSD4.9 + Zebra093b	fxp0	tr-b-agsw-01	fastethernet-0/4	FastEthernet	Multicast router
				fxp1	tr-b-agsw-02	fastethernet-0/4	FastEthernet	
114	tr-b-crsw-01	Foundry FastIron2402	03.0.00Tc1	e1	tr-b-cr-01	fe-0/0/1	FastEthernet	Backbone switch
				e2	tr-b-cr-02	fastethernet-1/1	FastEthernet	
				e10	tr-a-crsw-01	e10	FastEthernet	
118	tr-b-crsw-02	Foundry FastIron2402	03.0.00Tc1	e1	tr-b-cr-01	fe-0/0/2	FastEthernet	Backbone switch
				e2	tr-b-cr-02	fastethernet-1/2	FastEthernet	
				e10	tr-a-crsw-02	e10	FastEthernet	
98	tr-b-agsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-b-gw-01	gigabitethernet-0/2	FastEthernet	NOC internal switch
				fastethernet-0/2	tr-b-gw-02	fe-0/0/1	FastEthernet	
				fastethernet-0/10	tr-b-cr-01	fe-0/0/0	FastEthernet	
106	tr-b-agsw-02	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-b-gw-01	gigabitethernet-0/3	FastEthernet	NOC internal switch
				fastethernet-0/2	tr-b-gw-02	fe-0/0/2	FastEthernet	
				fastethernet-0/10	tr-b-cr-02	fe-0/0/0	FastEthernet	
122	tr-b-edsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-b-gw-03	fastethernet-3	FastEthernet	Upstream connection switch
				fastethernet-0/2	(NTT/VERIO)		FastEthernet	
				fastethernet-0/3	(IIJ)		FastEthernet	

(2) NOC-A

Two IPv4/IPv6 dual stack routes are added to support IPv6 in the access subsystem.

As with NOC-B, a dual stack router is installed to perform IPv6 backbone communications between the NOCs. This router also performs the role as a backup router for IPv4 backbone communications.

As with NOC-B as well, a separate IPv6 multicast router is also installed.

Table 7.3.2.3 shows the products making up NOC-A.

Table 7.3.2.3: Products Making Up NOC-A

No.	Host name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
1	tr-a-cr-01	Juniper M5	JUNOS 6.1R5	fe-0/0/0	tr-a-gsw-01	fastethernet-0/10	FastEthernet	Backbone router
				fe-0/0/1	tr-a-crsw-01	e1	FastEthernet	
				fe-0/0/2	tr-a-crsw-02	e2	FastEthernet	
2	tr-a-cr-02	CISCO 12404IR	IOS12.0(26)S	fastethernet-1/0	tr-a-agsw-02	fastethernet-0/10	FastEthernet	Backbone router
				fastethernet-1/1	tr-a-crsw-01	e1	FastEthernet	
				fastethernet-1/2	tr-a-crsw-02	e2	FastEthernet	
9	tr-a-ed-01	CISCO 7204VXR	IOS12.2(15)T	gigabitethernet-0/1	tr-a-edsw-01	fastethernet-0/1	FastEthernet	Access router
				gigabitethernet-0/2	tr-b-agsw-01	fastethernet-0/1	FastEthernet	
				gigabitethernet-0/3	tr-b-agsw-02	fastethenret-0/2	FastEthernet	
				fastethernet-2/0	HUB (HUB-v4-1)		FastEthernet	
10	tr-a-ed-02	GR2000-2B+	ROUTE-OS7B	fastethernet-0	tr-a-edsw-02	fastethernet-0/1	FastEthernet	Access router
				fastethernet-1	tr-b-agsw-01	fastethernet-0/2	FastEthernet	
				fastethernet-2	tr-b-agsw-02	fastethernet-0/2	FastEthernet	
				fastethernet-3	HUB (HUB-v6-1)		FastEthernet	
11	tr-a-ed-03	GR2000-2B+	ROUTE-OS7B	fastethernet-0	tr-a-edsw-03	fastethernet-0/1	FastEthernet	Access router
				fastethernet-1	tr-b-agsw-01	fastethernet-0/3	FastEthernet	
				fastethernet-2	tr-b-agsw-02	fastethernet-0/3	FastEthernet	
12	tr-a-mcast-01	HP DL320 R02	FreeBSD4.9 + Zebra093b	fxp0	tr-a-agsw-01	fastethernet-0/4	FastEthernet	Multicast router
				fxp1	tr-a-agsw-02	fastethernet-0/4	FastEthernet	
146	tr-a-crsw-01	Foundry FastIron2402	03.0.00Tc1	e1	tr-a-cr-01	fe-0/0/1	FastEthernet	Backbone switch
				e2	tr-a-cr-02	fastethernet-1/1	FastEthernet	
				e10	tr-b-crsw-01	e10	FastEthernet	
150	tr-a-crsw-02	Foundry FastIron2402	03.0.00Tc1	e1	tr-a-cr-01	fe-0/0/2	FastEthernet	Backbone switch
				e2	tr-a-cr-02	fastethernet-1/2	FastEthernet	
				e10	tr-b-crsw-02	e10	FastEthernet	
130	tr-a-agsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-01	gigabitethernet-0/2	FastEthernet	NOC internal

				fastethernet-0/10	tr-a-cr-01	fe-0/0/0	FastEthernet	switch
138	tr-a-agsw-02	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-01	gigabitethernet-0/3	FastEthernet	NOC internal switch
				fastethernet-0/10	tr-a-cr-02	fe-0/0/0	FastEthernet	
154	tr-a-edsw-01	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-01	gigabitethernet-0/1	FastEthernet	Access switch
158	tr-a-edsw-02	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-02	fastethernet-0	FastEthernet	Access switch
162	tr-a-edsw-03	Catalyst2950	IOS12.1(14)EA1	fastethernet-0/1	tr-a-ed-03	fastethernet-0	FastEthernet	Access switch

(3) Servers

Figure 7.3.2.2 shows the configuration of the server farm, and Table 7.3.2.4 lists the products that make up the server farm.

A new dual stack segment is set up below the new dual stack router in NOC-A. In this segment, an IPv6 service-providing reverse proxy server, combination DNS/mail servers supporting the dual stacks, and other servers are installed.

A new dual stack firewall is also installed in this segment, and a dual stack segment is provided below that as well. There, combination DNS/mail and other servers for use by the ISP users and internal operators are installed.

The above two segments contain various servers that are delivered by users in order to fulfill the wide varieties of services including peer-to-peer dependent applications and IPsec communication whose feasibility will be on the rise thanks to IPv6 deployment.

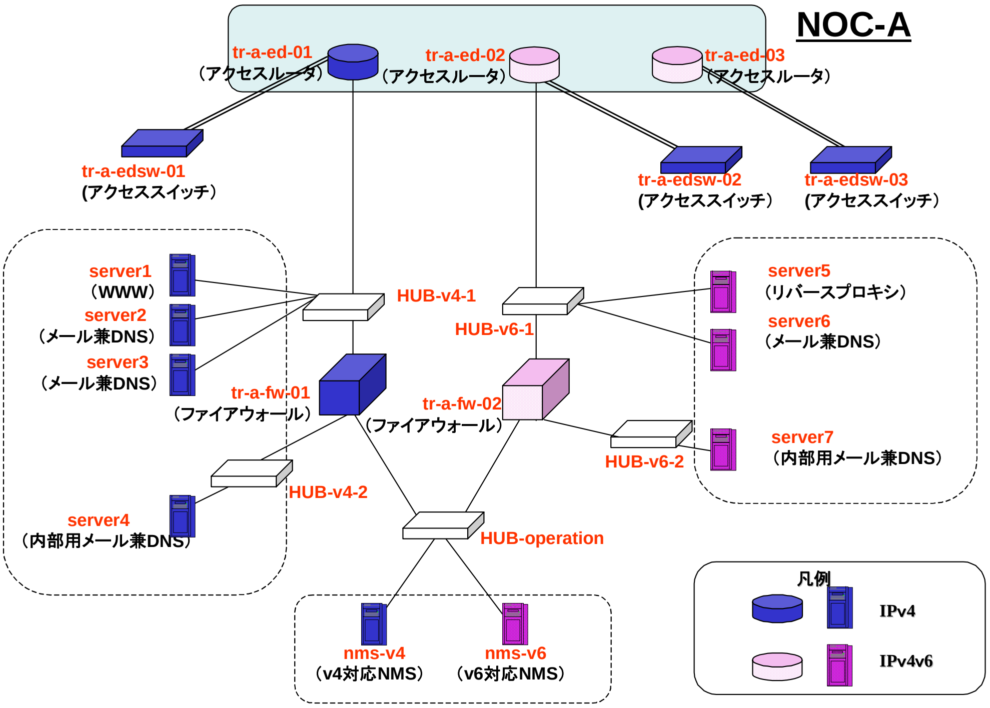


Figure 7.3.2.2: Physical Configuration of Servers (after Migration)

Table 7.3.2.4: Products Making Up the Servers

No.	Host name	Specification	OS	Interface	Associated device	Associated interface	Media	Notes
13	tr-a-fw-01	NOKIA-IP380	IPSO 3.7 FireWall-1 4.1	eth1	HUB (HUB-v4-1)		FastEthernet	Firewall
				eth2	HUB (operation)		FastEthernet	
				eth3	HUB (HUB-v4-2)		FastEthernet	
14	tr-a-fw-01	NOKIA-IP380	IPSO 3.7 FireWall-1 4.1	eth1	HUB (HUB-v6-1)		FastEthernet	Firewall
				eth2	HUB (operation)		FastEthernet	
				eth3	HUB (HUB-v6-2)		FastEthernet	
195	server1	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Web server
196	server2	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Combination public mail/DNS server
197	server3	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Combination public mail/DNS server
212	server6	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Combination public mail/DNS server
211	server5	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-1)		FastEthernet	Reverse proxy
202	server4	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v4-2)		FastEthernet	Internal combination mail/DNS server
226	server7	HP DL320	FreeBSD 4.9	fxp0	HUB (HUB-v6-2)		FastEthernet	Internal combination mail/DNS server
244	nms-v4	SunBlade 150	Solaris 9	eri0	HUB (operation)		FastEthernet	NMS server
245	nms-v6	SunBlade 150	Solaris 9	eri0	HUB (operation)		FastEthernet	NMS server

Logical Network Configuration

This subsection describes the logical configuration of the network for the model case ISP.

The following describes the configurations of Layer 2 (Ethernet layer) and Layer 3 (IP layer).

(1) Configuration of Layer 2

Figure 7.3.2.3 depicts the configuration of Layer 2 in NOC-A and NOC-B. FastEthernet is used within the NOCs. The circled numbers in the figure indicate the VLAN number.

The following discusses topics related to Layer 2 design in migrating to IPv6.

(a) Migrating the backbone subsystem to IPv6

In migrating the backbone to IPv6, a new IPv6-dedicated VLAN is installed. (This corresponds to a technique referred to as a line-sharing format by the Deploymnt WG Guidelines.) This also is a technique that has important hidden benefits, in that it enables the IPv6 traffic to be transferred logically isolated from the IPv4 traffic and enables IPv4 and IPv6 to be managed on the Layer 2 level separately and distinguishably. On the minus side, Layer 2 becomes a bit complicated due to the increase in the number of VLANs.

(b) Migrating the server subsystem to IPv6

The server segment is configured with a dual stack that does not particularly separate IPv4 and IPv6. (This corresponds to the technique referred to as a "dual format" by the Deploymnt WG Guidelines.) This approach is suitable for segments that contain dual stack servers or client PCs.

(c) Migrating the access subsystem to IPv6

As mentioned earlier, the transmission path of the access lines first encounters the physical access switch, then tag-VLAN is used to concentrate the logical segments on all access lines onto the link between the access switch and the access router, with the router providing the Layer 3 functions.

For the method to provide IPv6 access, there are three approaches. One is for the IPv4/IPv6 dual stack to provide IPv6 access, another is to provide access by using tag-VLAN separate IPv6 onto a single line, and the other is a native provisioning, in which a new native IPv6 connection line is set up. For all three approaches, both IPv4 and IPv6 protocols can be housed in the same router, or a different router can be selected to house each protocol. (The latter is assumed to be used where the existing IPv4 is housed in the access router in the interests of IPv4 stability, and IPv6 is housed in the newly installed IPv6 dual stack router.)

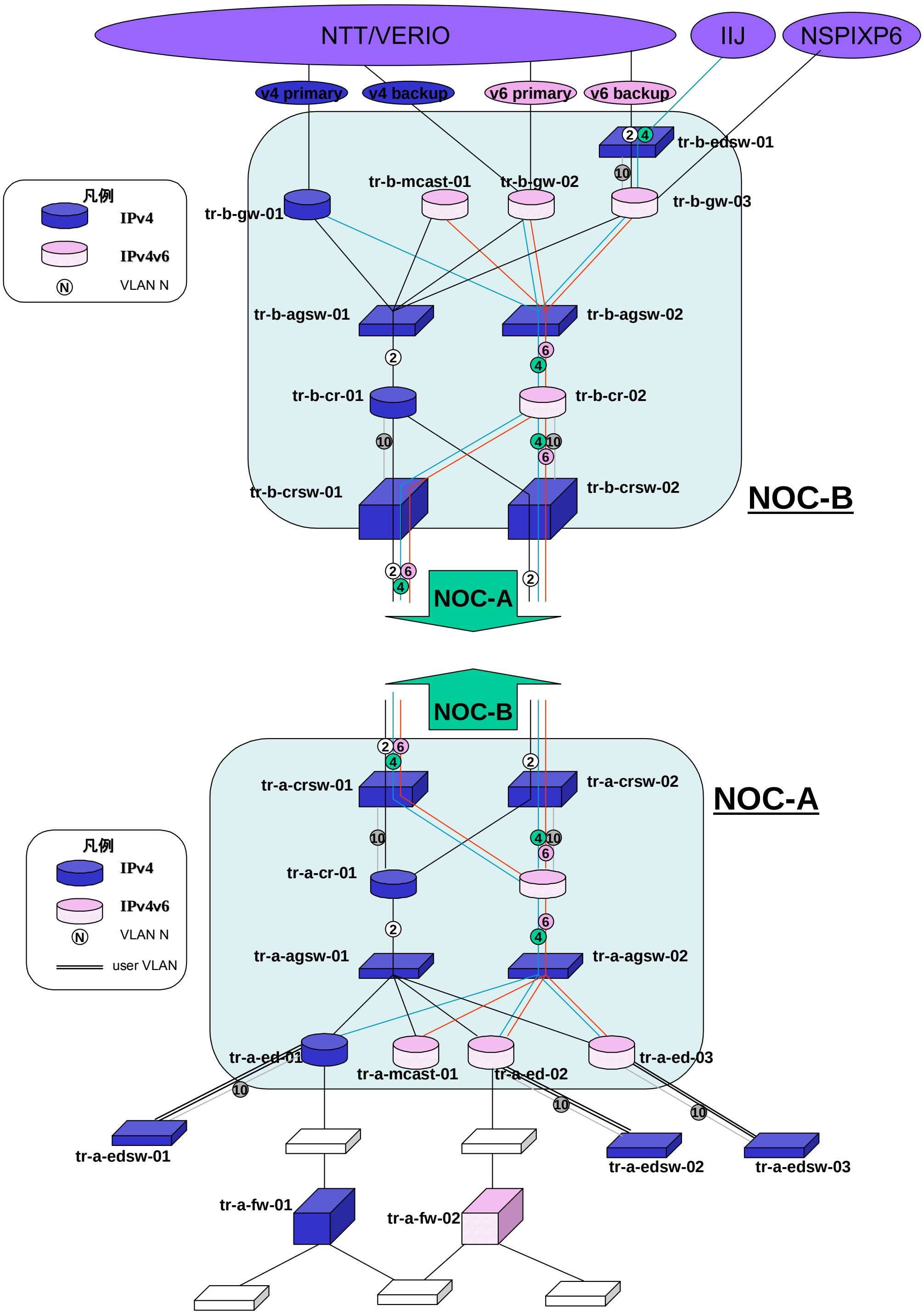


Figure 7.3.2.3: Configuration of Layer 2 (after Migration)

(2) Layer 3 IPv4 topology

Figure 7.3.2.4 depicts the IPv4 Layer 3 topology of this network.

OSPFv2 is used for the IPv4 routing protocol within the ISP network; the red numbers are the cost of OSPFv2 for the indicated link.

Compared with the topology before migrating to IPv6, the IPv4 topology has become a bit more complicated in line with the increased number of routers in use.

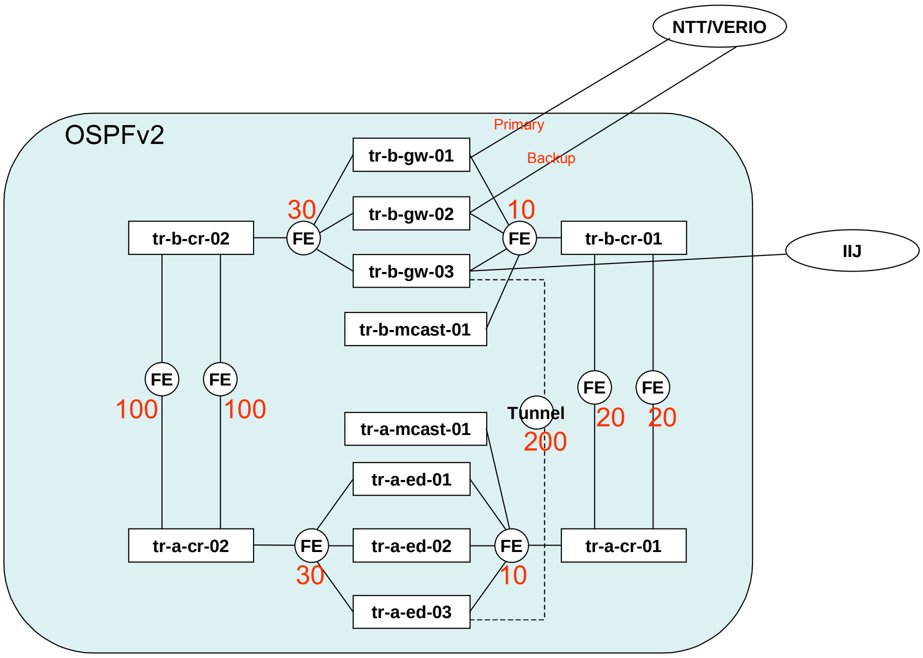


Figure 7.3.2.4: Configuration of IPv4 Layer 3 (after Migration)

Table 7.3.2.5 lists detailed information about the IPv4 routing

Table 7.3.2.5: IPv4 Routing Information (after Migration)

No.	Host name	Logical interface	Address	OSPFv2 (cost)	BGP Peer	Notes
1	tr-a-cr-01	lo-0	192.0.2.1	ON （1）	no bgp process (default routing)	Backbone router
		fe-0/0/0	192.0.2.129	ON (10)		
		fe-0/0/1.2	192.0.2.65	ON (20)		
		fe-0/0/2	192.0.2.69	ON (20)		
2	tr-a-cr-02	lo-0	192.0.2.2	ON (1)	no bgp process (default routing)	Backbone router
		fastethernet-1/0.4	192.0.2.137	ON (30)		
		fastethernet-1/1.4	192.0.2.73	ON (100)		
		fastethernet-1/2.4	192.0.2.77	ON (100)		

3	tr-b-cr-01	lo-0	192.0.2.3	ON （1）	no bgp process (default routing)	Backbone router
		fe-0/0/0	192.0.2.97	ON (20)		
		fe-0/0/1	192.0.2.66	ON (20)		
		fe-0/0/2	192.0.2.70	ON (100)		
4	tr-b-cr-02	lo-0	192.0.2.4	ON (1)	no bgp process (default routing)	Backbone router
		fastethernet-1/0.4	192.0.2.105	ON (30)		
		fastethernet-1/1.4	192.0.2.74.	ON (100)		
		fastethernet-1/2.4	192.0.2.78	ON (100)		
5	tr-b-gw-01	lo-0	192.0.2.5	ON (1)	EBGP NTT/VERIO (AS2914) IBGP tr-b-gw-02, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Upstream connection router
		gigabitethernet-0/2	192.0.2.99	ON (10)		
		gigabitethernet-0/3	192.0.2.107	ON (30)		
6	tr-b-gw-02	lo-0	192.0.2.6	ON (1)	EBGP (export; community 2914:480) (import: LocalPref: 90) NTT/VERIO (AS2914) IBGP tr-b-gw-01, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Upstream connection router
		fe-0/0/1	192.0.2.100	ON (10)		
		fe-0/0/2.4	192.0.2.108	ON (30)		
7	tr-b-gw-03	lo-0	192.0.2.7	ON (1)	IBGP tr-b-gw-01, tr-b-gw-02, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Upstream connection router
		fastethernet-1	192.0.2.101	ON (10)		
		fastethernet-2.4	192.0.2.109	ON (30)		
		tunnel-0	192.0.2.82	ON (200)		
8	tr-b-mcast-01	lo-0	192.0.2.8	ON (1)	IBGP tr-b-gw-01, tr-b-gw-02, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-a-mcast-01	Multicast router
		fxp0	192.0.2.102	ON (10)		
9	tr-a-ed-01	lo-0	192.0.2.9	ON (1)	IBGP tr-b-gw-01, tr-b-gw-02, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-a-mcast-01	Access router
		gigabitethernet-0/2	192.0.2.131	ON (10)		
		gigabitethernet-0/3	192.0.2.139	ON (30)		
		fastethernet-2/0	192.0.2.193	ON (10)		
10	tr-a-ed-02	lo-0	192.0.2.10	ON (1)	IBGP tr-b-gw-01, tr-b-gw-02, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-a-mcast-01	Access router
		fastethernet-1	192.0.2.132	ON (10)		
		fastethernet-2.4	192.0.2.140	ON (30)		
		fastethernet-3	192.0.2.209	ON (30)		
11	tr-a-ed-03	lo-0	192.0.2.11	ON (1)	IBGP tr-b-gw-01, tr-b-gw-02, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-a-mcast-01	Access router
		fastethernet-1	192.0.2.133	ON (10)		
		fastethernet-2.4	192.0.2.141	ON (30)		
		tunnel-0	192.0.2.81	ON (200)		
12	tr-a-mcast-01	lo-0	192.0.2.12	ON (1)	IBGP tr-b-gw-01, tr-b-gw-02, tr-b-gw-03, tr-a-ed-01, tr-a-ed-02, tr-a-ed-03, tr-a-mcast-01	Multicast router
		fxp0	192.0.2.134	ON (10)		

(3) Layer 3 IPv6 topology

The following describes the topology of the Layer 3 design after migrating to IPv6.

(a) Addressing

New IPv6 addresses must be obtained once IPv6 service starts. Considering that this network is for verification purposes and that satisfying the sTLA acquisition requirements is difficult, we accepted NLA address assignments from NTT/VERIO.

Of these assigned NLA addresses, NOC-A and NOC-B were both assigned /48. For the users accommodated under NOC-A, /48 is allocated keeping in mind the aggregation of assigned prefixes under NOC-A.

Each individual link used /64, as recommended in the Deployment WG Guidelines.

(b) Routing

As recommended by the Deployment WG Guidelines, OSPFv3 is being used as IGP. Note that the IGP cost is being established manually this time. (In the following figure, the red numbers indicate the cost of the associated link.)

For EGP, BGP4+ is being employed. In addition to the upstream connection, we are also performing NLA address broadcasting with Peer in IX as well.

(c) Redundancy

Although, for the IPv6 backbone, the native communications routes are single-plexed, backup of the native communications routes is provided with an IPv6 over IPv4 tunnel. An advantage to this technique is that, as long as an IPv4 route exists, backup communications can easily be provided.

Also, for the IPv6 upstream connection, two connection backups are provided.

(d) Multicasting

Because interconnects exhibit poor connectivity due to differences in router implementation when the network is configured, in the backbone, multicast connections are implemented by partially bypassing routers via tunneling.

Figure 7.3.2.5 depicts the IPv4 Layer 3 topology of this network.

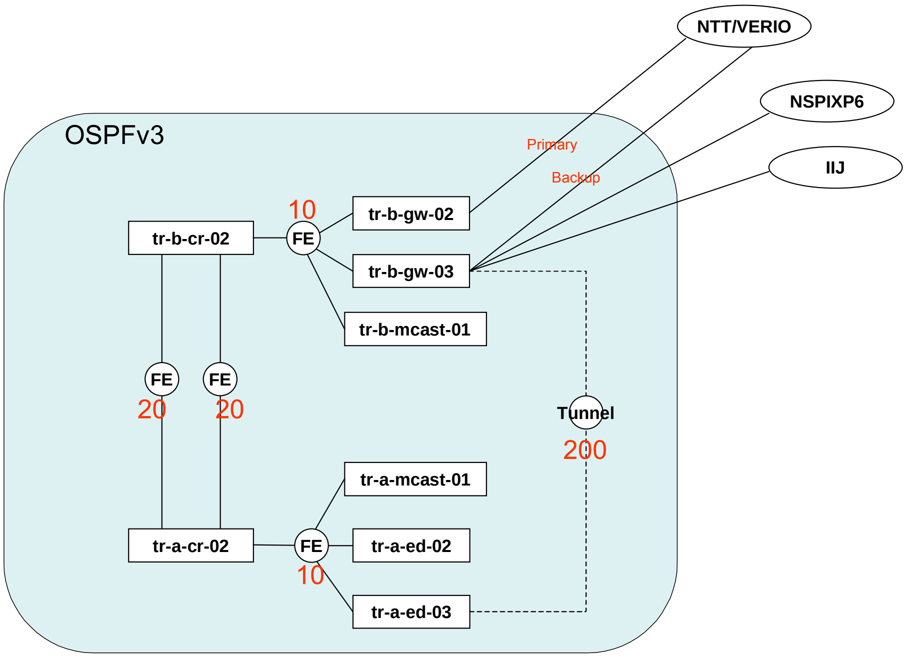


Figure 7.3.2.5: IPv6 Layer 3 Topology (after Migration)

Table 7.3.2.6 lists detailed information about IPv6 routing

Table 7.3.2.6: IPv6 Routing Information (after Migration)

No.	Host name	Logical interface	Address	OSPFv3 (cost)	BGP Peer	Notes
2	tr-a-cr-02	lo-0	2001:db8:6000::2	ON (1)	IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Backbone router
		fastethernet-1/0.6	2001:db8:6040::2	ON (10)		
		fastethernet-1/1.6	2001:db8:6000:1::2	ON (20)		
		fastethernet-1/2.6	2001:db8:6000:2::2	ON (20)		
4	tr-b-cr-02	lo-0	2001:db8:6000::4	ON (1)	IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Backbone router
		fastethernet-1/0.6	2001:db8:6010::4	ON (10)		
		fastethernet-1/1.6	2001:db8:6000:1::4	ON (20)		
		fastethernet-1/2.6	2001:db8:6000:2::4	ON (20)		
6	tr-b-gw-02	lo-0	2001:db8:6000::6	ON (1)	EBGP NTT/VERIO (AS2914) IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Upstream connection router
		fe-0/0/2.6	2001:db8:6010::6	ON (10)		
7	tr-b-gw-03	lo-0	2001:db8:6000::7	ON (1)	EBGP (export; community 2914:480) (import: LocalPref: 90)	Upstream connection router
		fastethernet-2.6	2001:db8:6010::7	ON (10)		

		tunnel-0	2001:db8:6000:3::7	ON (200)	NTT/VERIO (AS2914) IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	
8	tr-b-mcast-01	lo-0	2001:db8:6000::8	ON (1)	IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Multicast router
		fxp1	2001:db8:6010::8	ON (10)		
10	tr-a-ed-02	lo-0	2001:db8:6000::10	ON (1)	IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Access router
		fastethernet-2.6	2001:db8:6040::10	ON (10)		
		fastethernet-3	2001:db8:6040:1::10	ON (10)		
11	tr-a-ed-03	lo-0	2001:db8:6000::11	ON (1)	IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Access router
		fastethernet-2.6	2001:db8:6040::11	ON (10)		
		tunnel-0	2001:db8:6000:3::11	ON (200)		
12	tr-a-mcast-01	lo-0	2001:db8:6000::12	ON (1)	IBGP tr-a-cr-02, tr-b-cr-02, tr-b-gw-02, tr-a-ed-02, tr-a-ed-03, tr-b-mcast-01, tr-a-mcast-01	Multicast router
		fxp1	2001:db8:6040::12	ON (10)		

Applications

This subsection describes how IPv6 services are implemented in applications provided by this model case ISP. After describing the configuration required to support IPv6-compliant Web service, mail service, and DNS service, which are the main services provided by the ISP, the following discusses the ISP internal management system.

(1) Web

In this model case, Web service that supports IPv6 is implemented by setting up a separate dual stack reverse proxy. For the reverse proxy we are using Apache 2.
The following describes how requests for the Web content implemented in this case are processed.

When a client acquires Web content, the DNS server returns the Web server address as an IPv4 address (Record A), or returns the reverse proxy address as an IPv6 address (Record AAAA) when DNS name resolution is performed.

With IPv4 content acquisition, a content acquisition request is sent to this Web server address. With IPv6 content acquisition, the content acquisition request is sent to the reverse proxy address. Acting as an agent, the reverse proxy receiving this request obtains the content from the Web server and transfers it to the client. In this manner, both IPv4 and IPv6 Web service is performed.

Table 7.3.2.7 shows the configuration employed in this model.

Table 7.3.2.7: Web Service Configuration (after Migration)

No.	Host name	Specification	OS	Address	Application	Notes
195	server1	HP DL320	FreeBSD4.9	192.0.2.195	apache2.0.48	Web server
211	server5	HP DL320	FreeBSD4.9	192.0.2.211 2001:db8:6040:1::100	apache2.0.48	Reverse proxy

(2) Mail

In addition to the existing IPv4 mail servers, separate dual stack mail servers are installed for external communications and internal use to provide IPv6-compliant mail service.

The following explains communications between the external mail servers.

Communications between the internal mail servers and the external IPv4 mail servers is implemented as before on the legacy IPv4 server for external communications and the newly installed dual stack mail server is provided with backup functionality. Communication with the external IPv6 mail server is performed by a dual stack mail server for external communication. This means that, if needed, mail can be delivered between the existing IPv4 mail server for external communication and the dual stack mail server for external communication.

The following explains communication with the internal mail client in this case.

In this model, the existing internal IPv4 mail server handles communication requests from IPv4 mail clients, and the newly installed internal dual stack mail server provides backup functionality. Communication requests from IPv6 mail clients are handled by the internal dual stack mail server. Although, as before, the spool itself is maintained on the internal IPv4 mail server, IPv6 reception requests access the existing spool using ssh port transfer (as a simple POP3 proxy) from the internal dual stack mail server to the internal IPv4 mail server.

Table 7.3.2.8 shows the actual configuration.

Table 7.3.2.8 Configuration of Mail Service (after Migration)

No.	Host name	Specification	OS	Address	Application	Notes
196	server2	HP DL320	FreeBSD4.9	192.0.2.196	sendmail8.12.10	Public primary
197	server3	HP DL320	FreeBSD4.9	192.0.2.197	sendmail8.12.10	Public secondary
212	server6	HP DL320	FreeBSD4.9	192.0.2.212 2001:db8:6040:1::101	Sendmail8.12.10	Public secondary
202	server4	HP DL320	FreeBSD4.9	192.0.2.202	sendmail8.12.10 qpopper 4.0.5	For internal use
226	server7	HP DL320	FreeBSD4.9	192.0.2.226 2001:db8:6040:2::100	Sendmail8.12.10 sshd (port forwarding)	For internal use

Table 7.3.2.9 summarizes the mail distribution relationships.

Table 7.3.2.9: Mail Distribution Relationships (after Migration)

No.	Host name	Envelope_To	Method	Relay	Notes
196	server2	*	MX		v6trans.jp Primary MX (10)
		v6trans.jp	MailerTable	server4	
		*	Fallback MX	server6	
197	server3	*	MX		v6trans.jp Secondary MX (20)
212	server6	*	MX		v6trans.jp Secondary MX (30)
202	server4	v6trans.jp	Local		
		*	SmartHost	server2	
226	server7	*	SmartHost	server6	

(3) DNS

In addition to the existing IPv4 DNS servers, separate dual stack DNS servers are installed to provide IPv6-compliant DNS service.

The following explains the actual DNS server communication framework for this case.

When a local zone information query is received from an external IPv4 DNS server, either the legacy IPv4 DNS server or the newly installed dual stack DNS server responds. When a local zone information query is received from an external IPv6 DNS server, the dual stack DNS server responds. To implement this, both the IPv4 and IPv6 address of the new dual stack server must be registered as host information and the host information added to the NS record of the parent zone.

When a recursive DNS query request is received from an internal IPv4 client, the legacy IPv4 DNS cache server responds, and the newly installed dual stack DNS cache server provides backup functionality. When a recursive DNS query request is received from an internal IPv6 client, the dual stack DNS cache server responds. To implement this, the client-side resolver is set up to perform a DNS query to an arbitrary address from among the IPv4 addresses of the legacy IPv4 DNS cache server, the IPv4 addresses of the new dual stack DNS cache server, and the IPv6 addresses of this same server.

Table 7.3.2.10 shows the actual configuration.

Table 7.3.2.10: DNS Server Configuration (after Migration)

No.	Host name	Specification	OS	Address	Application	Notes
196	server2	HP DL320	FreeBSD4.9	192.0.2.196	bind8.3.7	Slave v6trans.jp. 2.0.192.in-addr.arpa. 0.6.8.b.d.0.1.0.0.2.ip6.arpa., etc.
197	server3	HP DL320	FreeBSD4.9	192.0.2.197	bind8.3.7	Zone master v6trans.jp. 2.0.192.in-addr.arpa. 0.6.8.b.d.0.1.0.0.2.ip6.arpa., etc.
212	server6	HP DL320	FreeBSD4.9	192.0.2.212 2001:db8:6040:1::101	bind9.2.3	Slave v6trans.jp. 2.0.192.in-addr.arpa. 0.6.8.b.d.0.1.0.0.2.ip6.arpa., etc.
202	server4	HP DL320	FreeBSD4.9	192.0.2.202	bind8.3.7	Cache server
226	server7	HP DL320	FreeBSD4.9	192.0.2.226 2001:db8:6040:2::100	bind9.2.3	Cache server

(4) Monitoring system

Table 7.3.2.11 describes the devices installed as the ISP monitoring devices.

Using legacy IPv4-compliant NMS, activity monitoring is realized using IPv4 PING polling and events are continuously monitored using SNMPtrap. In addition, by installing an NMS that supports dual stack, activity monitoring is realized using IPv6 PING polling. (The version of HP OpenView, which was installed as the NMS this time, enables use of the IPv6 PING polling monitoring and other functions through the addition of the separately available Extended Topology package.)

Table 7.3.2.11: Monitoring Configuration (after Migration)

No.	Host name	Specification	OS	Address	Application	Notes
244	nms-v4	SunBlade150	Solaris9	192.0.2.244	HP OpenView 6.4	
245	nms-v6	SunBlade150	Solaris9	192.0.2.245 2001:db8:6040:3::100	HP OpenView 6.4 + Extended Topology	

7.3.3 Evaluation

This subsection evaluates results after migrating this model case to IPv6.

As the main focus of this evaluation, in addition to evaluations of the migration from various people associated with this network, we also evaluate the migration cost and process as well. Lastly, we provide tips and other comments revealed by the actual migration of this model case.

Evaluation from a Building Standpoint

The migration approach described in Part 2 was able to reduce the workload on those building the network, because there was no need to set up temporary backups or synchronize switchover operations in order to minimize the time in which communications were cut off, due to the fact that no communications outages occurred in the IPv4 network while building the IPv6 network.

With respect to network stability as well, this migration approach did not cause any discernible adverse effects on the IPv4 network server services, confirming that migration by means of this scenario is an effective approach.

Evaluation from an Operator Standpoint

From the operational standpoint, the migration approach described in Part 2 increased the absolute number of devices due to the installation of new dual-stack devices, which made the IPv4 network topology a bit more complicated than the legacy network, and also increased the operational cost of log checks and other maintenance operations for the increased number of devices.

For the IPv6 network, a number of different links, such as native and tunnel bypass, were also introduced. Especially with respect to tunneling, it was determined that management costs increased somewhat from an operation viewpoint. In addition to the need for management to be aware of the IPv4 network topology, this increase was also caused because more man hours were required to isolate quality and reliability problems due to the dependence on IPv4, and because of limitations characteristic of tunneling.

Also, in expectation of greater reliability and to facilitate monitoring, the IPv4 and IPv6 segments were separated on the Layer 2 level. As a result, no problems occurred on the network during the operational phase either, and it was confirmed that this configuration could enjoy benefits such as being able to monitor traffic at the Layer 2 level with the increase in the number of VLANs.

For monitoring, complete IPv6 network support could not be implemented because SNMP support by IPv6 transport is incomplete. This means that, although the IPv4 functions must remain available for IPv6 service-dedicated devices as well, there are few IPv6-only devices at the present time, so this should not cause any significant cost increases.

Although this is outside the scope of Part 2, if providing IPv6 service, one must obviously set up a framework for handling IPv6 related issues, such as service management and customer management.

Evaluation from a User Standpoint

Because no communication outages occurred during operations, no problems occurred with the migration approach described in Part 2, even for those users whose usage profile would be severely impacted by a communications outage.

From the sense of providing a stable network as well, because backup for the legacy IPv4 communications continued to be provided for the user and IPv6 was protected with roughly the same degree of redundancy, no particular problems occurred for network stability either.

However, for those users who wish to use IPv6 on their own, depending on the ISP setup, a communication outage for the user may occur when swapping out routers or other work, so the user must confirm with the ISP beforehand.

Evaluation of Migration Costs

The migration approach described in Part 2 was able to hold down costs because it uses existing backup devices in the backbone subsystem for IPv6 communication. However, in the access subsystem, the installation of new dual stack routers produced various costs associated with the installation of new devices.

Also, IPv6 peering may reduce transit costs. Because the traffic in this test was not sufficient, we were unable to measure or extrapolate a reduction in the amount of transit traffic. However, normally, we know from experience with IPv4 that effective peering will draw off transit traffic to peers, an equivalent benefit would like occur here.

Tips

(1) Multicast implementation over a small MTU communications route

For the IPv6 Path MTU Discovery function, because some routers are implemented to not respond with an ICMP type 2 message (used for Path MTU Discovery) for a multicast packet, if the MTU can send a multicast packet over a relatively small communications route, such as a tunnel, it is assumed that Path MTU Discovering may not be effective and, when the distribution server is sending multicast packets, that sending a smaller MTU size is better.

7.3.4 Issues

This subsection describes findings and items of note obtained by actually implementing an IPv6 network in this model case ISP environment when performing actual communications.

Issues and Findings Related to IPv6, and Future Expectations

(1) State of IPv6 multicast implementation

It is assumed that, with IPv6, multicast-like communications will increase. At present, one must carefully select the device; because the implementation of IPv6 PIM-SM multicasting differs depending on the router platform, IPv6 multicasting may be impossible to implement among different types of equipment and there are devices that cannot transfer multicast packets over a tunnel interface.

Considering the hierarchical migration of multicasting, the significance demonstrated by this verification of multicasting via tunneling takes on a large significance. The key for multicasting to become popular is the proliferation of home routers equipped with multicasting functionality.

(2) IPv6 monitoring

Monitoring of the installed IPv6 network is essential. In addition to freeware that supports IPv6 monitoring, at present there are a number of commercial products that are sold as IPv6-compliant. Although the HP OpenView product, which has become the defacto standard in the network monitoring world, includes IPv6 monitoring functions and IPv6MIB acquisition functions, it does not yet provide support for IPv6 transport trap monitoring so, at present, it is not suitable for native monitoring of IPv6 networks.

There are also routers that are not equipped with the standard IPv6 MIB, so one must consider equipment selection carefully in cases where monitoring data on par with that reported for IPv4 is required.

(3) IPv6 support in virus checking functions

We are now seeing support for IPv6 by a number of applications, and environments in which IPv6 networks can be accessed without having to be aware of whether IPv4 or IPv6 are being put in place. Under these conditions, viruses that can propagate via IPv4 may be able to propagate into an IPv6 network. In particular, viruses that propagate via mail can easily spread into the network, regardless of whether it is IPv4 or IPv6.

Considering this situation, for our testing we developed and used the virus checking device InterScan GateWay Unit X300 for IPv6, which checks for viruses that spread using SMTP and POP3. Below, we discuss the findings derived from the results of this testing.

(a) SMTP/POP3 virus detection function

Using InterScan GateWay Unit X300 for IPv6 to search for viruses based on IPv6

SMTP/POP3 proxies, we confirmed that it is possible to detect viruses spread via IPv6 SMTP/POP3. Note that slight modification of the packaged application network APIs is needed to develop this function.

(b) Other issues of note

IPv6-compliant transparent proxies

Although by using a transparent proxy for IPv4 the virus detection function can be provided without setting the server as a proxy, because, on the operating system upon which development was based, the transparent proxy was not implemented on IPv6, the servers had to be set up individually. This means that future improvements must be made such that the user can complete this process without having to be aware of these settings.

IPv6 support by other anti-virus products

On migrating to IPv6, anti-virus products that support IPv6 are essential. In this migration demonstration test, we installed an appliance-type anti-virus product in the gateway subsystem that functions as the user's entrance to the Internet and verified its ability to combat viruses spread through SMTP and POP3. However, considering overall security, anti-virus functionality that targets only this gateway subsystem is insufficient. Anti-virus functionality that targets each layer is needed. Below we discuss IPv6 support provided in virus-protection products sold by Trend Micro, Inc., and the system changes required to support IPv6.

Layer divisions

Figure 7.3.4.1 shows the layer divisions.

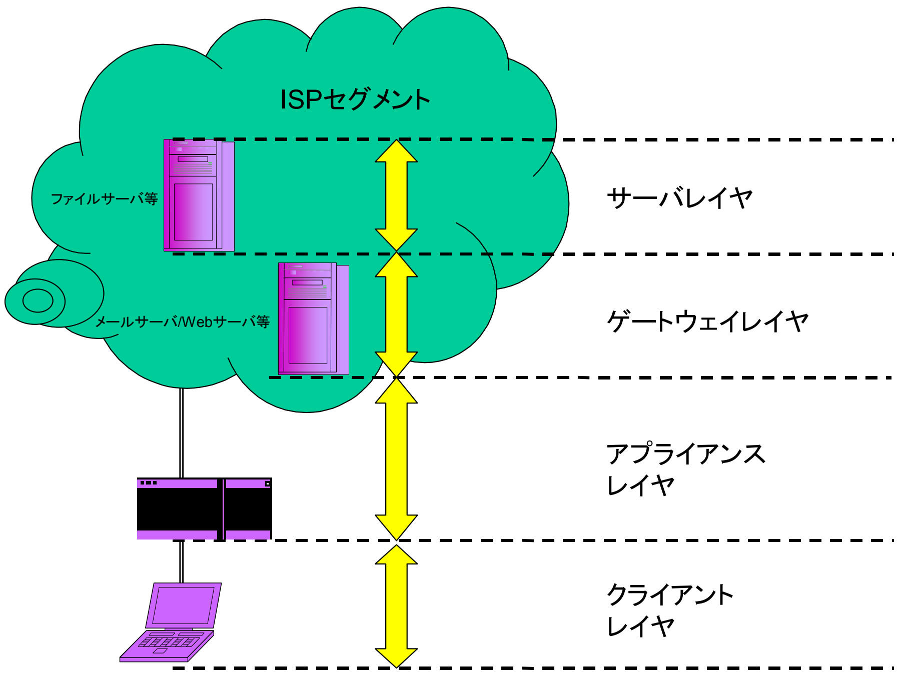


Figure 7.3.4.1: Layer Divisions

Current layer-targeted virus-protection products

Table 7.3.4.1 shows the virus-protection products for each layer that Trend Micro, Inc. currently sells and the functions that are implemented in an IPv4 environment.

Table 7.3.4.1: Virus-protection Products by Layer (IPv4)

Layer	Product name	Target of virus detection				
		Disk I/O	SMTP	POP3	HTTP	FTP
Server	ServerProtect	Yes	–	–	–	–
Gateway	InterScan Messaging Security Suite	–	Yes	Yes	–	–
	InterScan Web Security Suite	–	–	–	Yes	Yes
Appliance	GateLock X200	–	Yes	Yes	Note 1	–
Client	Virus Buster 2004	Yes	Yes	Yes	–	–

Note 1: GateLock X200 is for Web mail (AOL Mail, HotMail, Yahoo Mail, etc.)

Functions that operate in an IPv6 environment

Table 7.3.4.2 shows which function of the current products sold by Trend Micro Enterprises operate in an IPv6 environment.

Table 7.3.4.2: Virus-protection Software by Layer (IPv6)

Layer	Product name	Virus detection	Updatable [(Note 1)]
Server	ServerProtect	Yes	No
Gateway	InterScan Messaging Security Suite	No	No
	InterScan Web Security Suite	No	No
Appliance	GateLock X200	No	No
Client	Virus Buster 2004	Note 2	No

Note 1: Refers to all update functions including virus pattern files.
Note 2: Can only detect viruses using Disk I/O; it does not scan for SMTP/POP3.

System modifications by layer

Server layer

The server layer virus-protection product searches for viruses in files that are input to or output from any server, particularly the file server. Because the search is triggered by disk I/O, it searches for viruses even when installed in an IPv6 environment.

However, because the update function of the virus pattern file required for virus search does not operate in an IPv6 environment, the system must be modified to perform updates in an IPv6 environment.

If the search and the management servers are separate, as with ServerProtect for Windows NT, the subsystem linking the servers must also support IPv6.

Gateway layer

As you might expect from their features, virus-protection products for the gateway layer, such as InterScan Messaging Security Suite and InterScan Web Security Suite, are largely dependent on the network environment. This means that the virus search functions of gateway layer virus-protection products do not operate when installed in an IPv6 environment. Moreover, because many of the products provide virus scanning by being located in front of or behind the mail server, installation of an IPv6 gateway layer virus-protection product may block normal network operations.

As with the server layer, virus pattern updates do not work in an IPv6 environment.

Therefore, the system must be modified to install virus-protection products on the IPv6 gateway layer.

Appliance layer

The InterScan GateWay Unit X300 for IPv6 product that was used in this IPv6 migration demonstration test is a version of Trend Micro Inc.'s existing GateLock X200 product that has been modified to support IPv6.

As with the gateway layer described above, the system had to be modified in order to perform virus searching and virus pattern updates. Also, system modification had to be made to the router and other functions because it is an appliance product.

Client layer

As with server layer virus-protection products, in both IPv4 and IPv6 environments, client layer virus-protection products search for viruses when disk I/O is performed on a client PC. However, the system has to be modified because the portions of the client virus-protection product's functionality that search for viruses in an SMTP or POP3 session and that act as a firewall do not operate in an IPv6 environment, due to the fact that they are designed and implemented for an IPv4 environment.

As with the other layers, the system must be modified to handle virus pattern updates.

(4) Support for IPv6 in peer-to-peer sessions

Using the characteristics of the vast IPv6 global address space, it is expected that use of peer-to-peer applications will grow. In this test, we created and verified a hybrid-type peer-to-peer platform library for Windows XP, which is a platform for peer-to-peer applications, and a sample application named "competitive network mahjong."

Figure 7.3.4.2 shows the configuration of the test system.

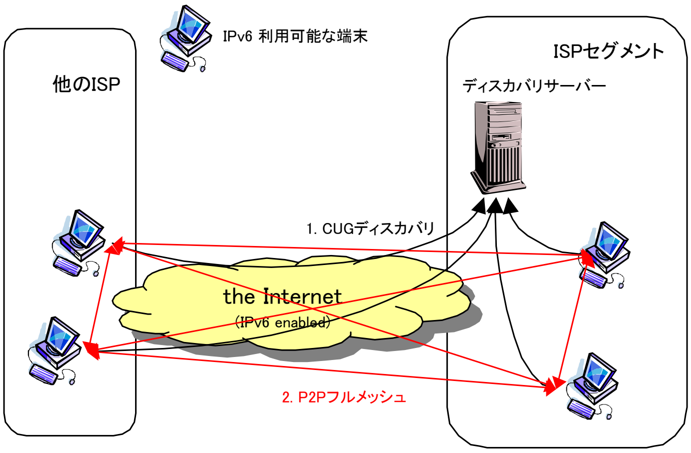


Figure 7.3.4.2: Test Configuration of the Peer-to-Peer Application

The peer-to-peer platform performs CUG discovery on the discovery server, performs a signaling link between the CUG terminals and creates a full mesh connection. (hybrid-type peer-to-peer connection)

Data communication on the hybrid-type peer-to-peer connection used in this test is performed directly between nodes. Closing data communication between nodes ensures that concentration of load on the server and line congestion does not occur. Benefits included the absence of the need to install load distribution technology required by Web services and easy expansion as a service model by collecting user group formation profiles and application usage profiles on the server.

When implementing the application, there is no need to consider

- UPnP-based NAT device control
- control of application protocol design

which gave rise to the current IPv4 Internet environment in which the private address space is employed for a variety of purposes. There are 5000 lines in the program that supports UPnP and NAT, and 3500 lines in the program that does not support UPnP and NAT. In other words, the effort required to implement migration to IPv6 can clearly be reduced, forming a basis for encouraging proliferation of peer-to-peer applications.

In this test, we installed an IPv6 Internet connection firewall (ICF) onto the operating system of the terminal, Windows XP, and started up a verification application while the peer-to-peer application was configured not to accept incoming communication from other terminals. This resulted in the application denying communication from the ICF signaling a request for CUG membership from other terminals, causing the formation of a CUG to fail. Because only per-port control is possible at the ICF, once a port is opened that port will accept connections from any host. To control connections from unintended terminals, a socket IP address must be obtained at the application layer and authentication performed based on that address. Because this technique is not typically provided for such implementations, at this time it has to be implemented separately in each application.

Control of an ICF-included firewall is a problem not only for applications on nodes; the security policy of the entire network protected by that firewall must take it into account as well. This means that, not only must one establish a method of notification to individually approve communications from outside, but a system must be established to centrally manage control of the firewall on the network.

(5) Support for IPv6 in streaming functions

As one type of content offered by the ISP, we investigated provisioning of streaming communications. This subsection summarizes the findings obtained at this time.

(a) Modification of MTU size

When a multicast packet was sent from a distribution server, a behavior occurred whereby the Path MTU Discovery function did not operate effectively. (see 7.3.3 Tips for details)

To overcome this, we forcibly changed the size of the MTU in order to guarantee that packets on all multicast routes were transferred.

Specifically, we entered the netsh command at the command line prompt and then entered the command set interface "local-area-connection" mtu=1280.

On the other hand, it was pointed out that even if we enabled the Path MTU Discovery function for multicast packets operating over IPv6 on all nodes, when there was a large number of users the response processing alone caused a great increase in the distribution server load. In such cases, although it is possible to avoid such a situation by turning off the Path MTU Discovery function on the distribution server side, and setting a static MTU as we did this time, the problem of a much larger overhead compared with IPv4 persists.

(b) Disabling of IPv6 ICF (Internet Connection Firewall)

Because IPv6 ICF was automatically configured when Windows Update for Windows XP installed Advanced Networking Pack for Windows XP, a situation occurred whereby multicast data could not be received. Therefore, to receive multicast data, one must explicitly configure the settings to disable the ICF.

Specifically, enter the netsh command at the command line prompt, and then enter the command firewall set adapter "local-area-connection" filtering=disable.

(6) Support for IPv6 in IPsec

With IPv4, even in private segments under control of NAT, global addresses are expected to be used more as IPv6 is increasingly adopted. With this type of change in usage format, security protection techniques will need to be examined once again. In this test, we examined the use of IPsec using MyNetManager, which is a security policy mechanism for central management and distribution from a policy server. The following describes the findings obtained from this examination.

(a) Firewalls and IPsec

Although the findings revealed that the secure end-to-end communications provided by IPsec is a realistic enough solution, we found that the opposite side of the benefit of network accessibility ensured by IPv6 means that, unless all communication is premised on IPsec, all terminals may be subject to a worm attack. For such situations, we believe that using a combination of firewall functions and IPsec to block worms would be effective and development of a mechanism that links IPsec with a firewall will become a topic of discussion. Role-sharing between the firewall and IPsec could be as follows:

- Firewall

  Enables one to restrict addresses, ports and protocols used for communication between a managed network and the outside. For example, this could protect the intranets and LANs of local governments and enterprises from invalid packets, but cannot provide control at the terminal level when mobile environments that can modify addresses dynamically are included.

- IPsec

  This ensures security at the terminal level. To authenticate terminals and users, automatic distribution of policies that use certificates would enable authentication between terminals. This protects against attacks on terminals and ensures encrypted communications between terminals that have authenticated each other.

(b) Encryption and IPsec

Although compared with SSL and other encryption methods IPsec has the benefit of being applicable to any type of communication, IPsec has a bit larger performance overhead than implementing encryption directly in the application. As such, we had to heed the following points when we examined the installation:

- If encryption must be performed for a variety of applications (file transfer, audio communications, video communications between individuals, etc.), using IPsec to ensure secure communications is effective.
- For cases in which the remote side must be authenticated at the application level, or it is important for both sides to ensure both performance and security (such as video distribution services needed by copyright administrators), implementing encryption in the application is more effective.

(c) IPsec policy configuration management

Because installation of IPsec requires control by means of appropriate policy settings for each terminal, administration cost increases are an issue. The MyNetManager product that we used in this test provides a way to configure the IPsec settings for each terminal automatically, by setting the policies for the terminals on the server and automatically distributing them from there. If there are *n* terminals, this results in a configuration and management workload of 1/*n* compared to when this product is not used. In other words, this mechanism can dramatically reduce the configuration management cost for each terminal, which is an issue that results from one of the advantages afforded by IPv6, namely, the assurance of secure, end-to-end communications from terminal to terminal, and is a realistic solution.

(7) Support for IPv6 in SIP functions

Attention is currently focused on SIP for IP telephony and other implementation techniques. In the following, we examine SIP-based IP telephony in an IPv6 environment.

Testing of IP telephony verification (SIP) confirmed the interconnectability of various segments and that the audio quality was at a practical level. However, a number of issues become evident when considering this from the viewpoint of encouraging the diffusion of IP telephones based on IPv6 to users connected over IPv4.

(a) Automatic port filtering configuration

When communicating with software for IP telephony that we used in this testing, we had to open a large number of ports. To encourage future use, functions to dynamically open ports as needed must be implemented in both the applications and network devices.

(b) Telephone directory

When using IP telephony, the user must already know the remote URI. This did not present a significant problem in this testing because it was used in a small, closed community; however, a directory service that permits information retrieval while protecting the security of private information will be vital in cases where it is used on a large scale in open environments after migration to IPv6.

(c) SIP security

Although one must log into the SIP server when communicating using IP telephony software, since communication is not encrypted, a technique to confirm membership may be employed. To do so, SIP security may have to be combined with IPsec or other security protocols.

8. Conclusion

8.1 The Deployment Scenarios that were Demonstrated

The deployement scenarios that were applied here can be broadly classified into two major types, independent merging and staged replacement. During introduction of IPv6, deployement policy should basically be to exclude effects on both the segments and existing services in the layer that can be called the parent.

Currently, the independent merging scenario provides a roadmap for migration to IPv6 when building a new IPv6 environment using particularly critical components, such as the upstream connection, firewall and server. The segments in which this was demonstrated were local governments, small- and medium-sized enterprises and wireless LAN access.

The staged replacement scenario enables migration to IPv6 in cases in which the products installed in the existing environment already are compatible with a dual approach and is relatively easy when combined with installation of new applications. The segments in which this was demonstrated were local governments, large enterprises and ISPs.

However, for all segments, to balance cost rationalization and effects on existing service in all segments, both scenarios were employed on a partial basis. For the enterprise network administrators and system integrators to whom this is mainly targeted, it is obvious that we believe scenarios must be applied on a case-by-case basis using this demonstration as a base, depending on the products that will appear in the future and the configuration of the existing environment.

On the other hand, the home segment was noteworthy, in that the introduction of services and products that support IPv6 revealed progress toward IPv6. The reason for this is that simply using IPv4/IPv6 dual service in the ISP meant that the network had been migrated to IPv6, due to fact that the network configuration is simple. By installing new IPv6-compliant devices and setting up the screens for managing these devices, the end user is able to begin using IPv6 without having to be aware of any changes.

8.2 General Considerations

What became clear as we proceeded with the actual verification testing is that differences in migration costs arose from the installation and operational aspects depending on the applications and devices that were used. Events that were discovered by combining technologies and approaches, such as the need to tune settings to enable operations, being compelled to take other migration approaches because of functional limitations and unexpected operation dependent on the address that was used are matters for improvement as we proceed with the migration, as well as the significance of this demonstration.

As one example, although tunneling, which is a technology used to migrate to IPv6, is typically used to reduce the cost of installing IPv6-enabled devices, unforeseen installation and operational costs arose depending on the devices and applications used. In other words, considered in its entirety, the cost of the tunnel approach might, in fact, be more expensive and, from the cost aspect, creating a dual network might be more advantageous.

The model environments of the segments that were migrated to IPv6 were set up with typical configurations and conditions in order for their scope of application to be as broad as possible. Moreover, because IPv6 support is already provided in many currently available products, they did not include a faithful reproduction of the model environments before migration, including legacy business systems that are currently in use.

Two points are needed to promote the further proliferation of IPv6.

- Continue to overcome the technical issues discussed in the following section, expand the variation of environments, devices and applications targeted for migration and faithfully reflect the guidelines.
- Quantify the installation benefits and market size, and enable expansion of the solution results to surrounding areas.

In Part 2, we made great efforts to clearly state the specifications and versions of each device and application that we actually used and provided the settings for the devices in a separate paper. Thus, the information shown in this case study can be used as reference material when introduction of IPv6 is further examined by enterprise network administrators and system integrators in future.

8.3 Technical Issues

Although the IPv6 deployement guidelines used in this verification testing clarified procedures and methods that could be used for IPv6 deployement, it is also clear that there is a number of technical issues that cannot be realized at the present time that are needed for IPv6 to spread and to make feasible more advanced use of IPv6. To promote the future proliferation of IPv6, these barriers must be removed. The following summarizes the main issues.

- Peer-to-peer communications security

  There is large number of SIP communication cases in which peer-to-peer applications are used. However, because SIP itself does not include an encryption mechanism and a wide range of ports is used for communication, a dynamic port filtering mechanism is needed via either a firewall or a personal firewall.

- Linking of IPsec with firewalls and policy management

  When a user who belongs to an organization performs end-to-end IPsec communications, the mutual consent of the users alone is insufficient from the standpoint of security policy. The administrator must have a mechanism to open and close the firewall entrance and manage and control the user's IPsec communication according to a specific policy.

- Terminal address management

  In order for the network administrator to easily manage and identify the address of a user terminal, in addition to the current automatic configuration of stateless addresses, the user must also have a statefull mechanism.

- DNS

  In the current IPv6 environment, an automatic discovery method has not been implemented in the DNS server, and there are few transport name resolution implementations. More such implementations must be made available in future.

- Multicast

  Increased availability of multicast routing protocol (PIM-SM) implementations in routers is needed (in home routers, support for tunnels is desired first), as well as support by firewalls for multicast packets.

- Application operations

  Establishment of operational guidelines for dual stack applications and proliferation of implementations based on these guidelines are needed. In particular, due to its employment in IP telephony, SIP is seen as a critical application protocol, and guidelines and implementations are required at an early stage.

- Virus-protection

  Even in the appliance-type applications that we used, it is necessary for all varieties of virus check products (server, gateway, client) to provide support

IPv6 and to detect and eliminate viruses regardless of whether IPv4 or IPv6 is used.

- Mobile IPv6

  For mobile IPv6, which is one of the hallmarks of IPv6, we have come to a stage at which standardization of the specifications can be seen. We now need to quickly see implementations of it in devices, and demonstration testing of it in linkage with applications.

- Support for IPv6 by other appliance products

  Although there are some products that provide IPv6 support, such as firewalls, IDSs, load balancers, accelerators and network management equipment, from a functional and performance standpoint many products can be improved and, even from the standpoint of increasing the number of solutions available, there is a need for a more substantial lineup of products that support IPv6.

Final Note

Forthcoming IPv6 Deployement Guidelines

We plan to publish the next update of the guidelines by March 2005.

As stated in the "introduction," we hope to reflect the demonstrated, concrete findings we obtained in Part 2 in the next version of Part I (Next Stage IPv6 Deployement Guidelines Selected by the IPv6 Promotion Council).

The Asia Pacific IPv6 Task Force formed in February 2004 established a Guideline working group, and decided that Part 2 would use it as a springboard for discussion.

In addition to the above, the IETF v6ops working group has unveiled deployement scenarios for the enterprise, ISP, mobile and home segments in various RFCs. The main targets were device, application and protocol developers and so focused on their development period and orientation guidelines. In contrast, except for a few segments, Part 2 targeted those who actually are building and operating networks, and provided guidelines on what they should do and how they should think. Due to the differences in the target readership, we plan to proactively work toward integrating those parts of Part 2 that can contribute to the RFCs into the IETF as well.

In the end, those who provide equipment on an agent basis and also solutions will continue to efficiently make progress toward innovations in IPv6 and we expect system integrators will independently develop IPv6 deployement guidelines that are matched to such equipment and solutions. We hope that Part 2 will become a reference for the guidelines published by these system integrators.

2004 Version IPv6 Deployment Guideline Summary

Issued in June 2004

Issued by	IPv6 Promotion Council of Japan
Inquiries	wg-dp-comment@v6pc.jp
URL	http://www.v6pc.jp/